МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра "Компьютерные технологии"

«Допущен к защите»
Заведующий кафедрой _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: "Разработка физической безопасности и контроля доступа для здания"

Специальность 5В070400 - Вычислительная техника и программное обеспечение

Выполнил (а) Попов А.Р. (Фамилия и инициалы) БВТ-10-03 (группа)

Научный руководитель Майлыбаева А.Ж., ст. препод. (Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ергалиева З.Д., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ергалиева «14» мая 20 14 г.
(подпись)

по безопасности жизнедеятельности:
Дуйсебаева Н.Г., д.х.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «14» 05 20 14 г.
(подпись)

по применению вычислительной техники:
Майлыбаева А.Ж., ст. препод.
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Нормоконтролер: Тусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
_____ «15» мая 20 14 г.
(подпись)

Рецензент: _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет "Информационные технологии"
Специальность "Вычислительная техника и программное обеспечение"
Кафедра "Компьютерных технологий"

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Попов Александр Дмитриевич
(фамилия, имя, отчество)

Тема проекта Разработка физической безопасности и контроля доступа для здания.

утверждена приказом ректора № 115 от «24» сентября 2013 г.
Срок сдачи законченной работы «7» июля 2014 г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

Документация Cisco, книги по проектированию безопасного и контроля доступа для здания

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

1. Аналитическая часть
2. Конструкторская часть
3. Общая сетевая часть предприятия
4. Анализ потенциально опасных и вредных производственных факторов.
5. Технико - экономическое обоснование

Перечень графического материала (с точным указанием обязательных чертежей)

В данной работе содержится 49 рисунков и 21 таблица

Рекомендуемая основная литература

1. Барухов, В.С. Современные технологии безопасности ВС Барухов, В.В., Водопьянов. - М.: Нолидж, 2000. - 496 с., ил.
2. Башин А.В. Видеонаблюдение как часть интегрированной системы безопасности. - Конкурент, 1999. - №6. - С. 55-59
3. Документация Cisco.
4. З.Ф. Ураксеев, Г.И. Бохонов. Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В074600 - Вычислительная техника и программное обеспечение. Алматы: АУЭС, 2013-40с.
5. СНиП РК 2.04-05-2002 Естественное и искусственное освещение. Строит. нормы и пр-а. Агентство по делам строительства РК. - Астана, 2002. - 52с.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Экономика	Ураксеева З.Ф.	25.04-12.05.14	Ураксеева
БЖД	Приходько Н.Г.	11.04 - 11.05.14	
Основная часть	Бакпенбаева А.Ж.	11.04-20.05.14	
Нормоконтроль	Тусупов Д.М.	15.05.2014	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1.	Сбор необходимого материала	15.03.14.	
2.	Обследование объекта и его описание	01.04.14	
3.	Построение предварительных схем сетей предприятия	14.04.14	
4.	Разработка алгоритмов безопасности	21.04.14	
5.	Разработка внедрения сетевых датчиков безопасности	26.04.14	
6.	Отладка всех датчиков	01.05.14	
7.	Технико-экономическое обоснование	06.05.14.	
8.	Безопасность жизнедеятельности	14.05.14.	

Дата выдачи задания «3» марта 2014 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Тютюнникова А.Н.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Попов А.Д.
(подпись) (Фамилия и инициалы)

Аннотация

Данный дипломный проект посвящен разработке и реализации комплекса физической безопасности и контроля доступа для здания. Произведен анализ злоумышленника. В общей сфере предприятия для обеспечения должной безопасности, было рассмотрено и внедрено большое количество датчиков производителя Cisco удовлетворяющие нашим запросам.

Дано технико–экономическое обоснование проекта, произведен расчет затрат на разработку физической безопасности, рассмотрены аспекты, связанные с обеспечением безопасности и оптимальных условий труда на рабочем месте.

Аңдатпа

Бұл дипломдық жоба физикалық қауіпсіздік кешенін әзірлеу мен жүзеге асыруға және ғимаратқа қатынау жүйесін бақылауға арналды. Қаскүнемдерге талдау жасалды. Кәсіпорынның жалпы саласында тиісті қауіпсіздікпен қамтамасыз ету үшін біздің сұраныстарымызды орындаушы Cisco өндірісінің бергіштерінің үлкен көлемі қаралды және енгізілді.

Жобаның техника-экономикалық дейектері берілді, физикалық қауіпсіздіктерді әзірлеуге шығындар есебі жүргізілді, жұмыс үстелінде еңбек қауіпсіздігімен және оңтайлы жағдайлармен қамтамасыз ету аспектілері қарастырылды.

Abstract

This thesis project focuses on the development and implementation of a range of physical security and access control for the building. The analysis of the attacker. A total area of the enterprise to ensure adequate security was considered and implemented a large number of sensors manufacturer Cisco satisfy our requests.

Given the feasibility study of the project , calculated the cost of development of physical security, discussed issues related to safety and optimal conditions in the workplace.

Содержание

Введение

Физическая безопасность (защита) организации – это совокупность правовых норм, организационных мер и инженерно–технических решений, направленных на защиту важных интересов и ресурсов предприятия (объекта) от угроз злоумышленных противоправных действий физических лиц (нарушителей). Она включает в себя силы службы безопасности и охраны объекта, комплекс инженерно–технических средств охраны, режим, установленный на объекте. Система физической защиты не должна препятствовать нормальному функционированию организации, ее технологическим процессам.

В современных условиях сложной криминогенной обстановки в мире вопросы обеспечения безопасности населения и промышленных объектов приобретают особую актуальность. Особую опасность для крупных промышленных объектов представляют злоумышленные несанкционированные действия физических лиц (нарушителей): террористов, диверсантов, преступников, экстремистов. Результаты их действий не предсказуемы: от хищения имущества до создания чрезвычайной ситуации на объекте (пожар, разрушение, затопление, авария, и т.п.).

Одной из эффективных превентивных мер по обеспечению безопасности важных промышленных объектов является создание автоматизированной системы охраны от несанкционированного проникновения физических лиц – системы физической защиты (СФЗ).

Современные СФЗ в корне изменили тактику охраны объектов. В таких системах нет необходимости в организации постовой службы на периметре объекта; вместо этого создаются дежурные тревожные группы, которые начинают немедленные действия по нейтрализации нарушителей после получения сигнала тревоги на центральном пульте управления СФЗ. В них сведено до минимума влияние человеческого фактора и достигается высокая эффективность защиты объекта при минимальном количестве личного состава сил охраны.

В настоящее время рынок услуг все больше и больше завоевывают частные охранные предприятия (ЧОП). Эти фирмы предоставляют услуги охраны собственности другим предприятиям, а так же частным лицам. Важнейшей задачей частных охранных предприятий и работающих в нем сотрудников по защите информации является сохранение и защита от распространения.

Чем выше уровень (или эффективность) безопасности, тем выше вероятность сохранения всех ценностей объекта от хищений или уничтожения. Уровень безопасности, в свою очередь, в основном зависит от того, насколько полно и правильно была разработана комплексная система защиты информации на предприятии. Другим немаловажным фактором является правильно подобранная система видеонаблюдения, которая усиливает надежность комплексной системы безопасности организации.

Целью дипломной работы является проведение анализа объекта с последующим проектированием системы комплексной защиты информации в организации с разработкой системы видеонаблюдения IP–камер Cisco, датчиков сторонних поставщиков, систем контроля доступа Cisco.

В рамках единой политики безопасности организации физическая безопасность является ее основным структурным элементом, направленным на сохранение собственности, жизни и здоровья персонала, финансовых ресурсов. Концепцией физической безопасности организации предусматривается:

– определение возможных угроз функционированию объектов Компании, вероятных исполнителей угроз (нарушителей);

– определение наиболее уязвимых мест на объекте, т.е. вероятных предметов защиты;

– оценка уязвимости предметов защиты Компании, т.е. соответствия существующей системы безопасности выявленным угрозам;

– разработка предложений и проведение необходимых мероприятий по обеспечению безопасности объекта.

1. Аналитическая часть

1.1 Методика построения корпоративной системы защиты информации

Задачу построения адекватной сегодняшней обстановке системы безопасности объекта можно условно разбить на две основные части: организационная и техническая.

Опыт ученых–практиков, разрабатывающих концептуальные решения по созданию СФЗ на особо важных объектах различных ведомств и располагающих большим объемом аналитического материала, позволяет сделать некоторые выводы о тенденциях, складывающихся в сфере создания/модернизации СФЗ.

Повышение эффективности организационной части в деле обеспечения безопасности объекта как наиболее операбельного фактора нельзя принизить ни в коем случае. Он был и еще достаточно долго останется на большинстве объектов ключевым звеном. Но речь сейчас лишь о том, чтобы снизить нагрузку, приходящуюся на долю сотрудников охраны, повысив при этом их защищенность и эффективность всей системы в целом.

Обоснование и оптимизация структуры и функциональных характеристик системы, разработка требований и рекомендаций к ее элементам являются основным содержанием и целью деятельности, которая в настоящее время формируется как научно–методическое сопровождение создания СФЗ.

Научно–методическая и аналитическая работа в рассматриваемой области складывается из совместной деятельности:

– администрации и служб безопасности объектов;

– специализированных организаций.

Эта работа включает в себя:

– проведение полного обследования объекта информатизации;

– определение класса защиты объекта, категорирования помещений, определение (задание) критерия эффективности создаваемой или модернизируемой СФЗ;

– выделение наиболее вероятных угроз и определения модели потенциального нарушителя (его основные характеристики и цели), анализ уязвимости объекта, оценку эффективности существующей и создаваемой СФЗ;

– разработку концептуального решения по созданию (модернизации) СФЗ, требований к составу и функциональным характеристикам СФЗ;

– выбор и оптимизацию системы;

– актуализацию концепции создания СФЗ при изменениях угроз и условий функционирования объекта и его СФЗ.

Полное обследование объекта производится для получения наиболее полного анализа характеристики объекта. Проводят, как организация–заказчик, так и организация–разработчик. Это одна из наиболее важных стадий пред

проектной подготовки.

Задача решается экспертными методами путем определения видов и масштабов ущерба, который может возникнуть в случае реализации угроз. Результатом является отнесение объекта к соответствующей категории, что, в свою очередь, определяет общие требования к СФЗ и позволяет задать количественные критерии эффективности СФЗ, необходимые в дальнейшем для оценки системы.

В мировой и отечественной практике основной критерий имеет интегральный характер и количественно выражается величиной вероятности пресечения СФЗ и действий нарушителя до достижения им своей цели при наиболее благоприятных для него условиях (так называемый «пессимистический подход»).

Категорирование объектов само по себе не решает проблемы обеспечения безопасности и лишь позволяет установить степень потенциальной опасности и общие требования к системе физической защиты каждого конкретного объекта.

Следующим шагом должно быть определение степени соответствия существующей СФЗ объекта требованиям, предъявленным в результате категорирования. Для этого необходимо проведение анализа уязвимости объекта. Создание/модернизация систем обеспечения безопасности без анализа ситуации на объекте защиты (анализа уязвимости объекта) и научно обоснованных рекомендаций может привести, например, к тому, что не будут учтены какие–то важные угрозы, а в создание/модернизацию системы безопасности будут вложены средства, превышающие реально необходимые.

Анализ уязвимости объекта выполняется экспертными методами и/или методами имитационного моделирования и включает в себя:

– расчет интегрального показателя и комплексную оценку эффективности существующей СФЗ (при установленных видах угроз и приоритетах целей защиты) путем сравнения полученных расчетных данных с заданными критериями;

– разработку мер по достижению заданных критериев;

– оценку (подтверждение) эффективности этих мер.

Меры по достижению заданных критериев эффективности являются, по сути, требованиями к структуре и функциональным характеристикам создаваемой или модернизируемой СФЗ и тем самым логически завершают этап разработки концепции создания системы.

Результатами этого этапа являются:

– рекомендации по структуре и содержанию организационно–распорядительных документов об обеспечении безопасности объекта;

– проект организационно–штатной структуры и рекомендации по организации сил охраны объекта;

– требования по назначению к инженерно–техническим средствам и системам (ИТС), входящим в СФЗ; эти требования являются основой для разработки технического задания на проектирование СФЗ.

И руководящие документы, и складывающаяся практика одинаково

определяют субъект анализа уязвимости. Анализ должен проводиться с привлечением специализированных организаций, имеющих в своем составе квалифицированных специалистов в различных областях знаний и располагающих специальным программно–методическим обеспечением. Только при таком подходе можно обеспечить объективность и высокое качество анализа уязвимости и создать эффективную систему обеспечения безопасности, экономически целесообразную для объекта защиты.

1.1.1 Разновидности аналитических работ по оценке защищенности

Аналитические работы в области информационной безопасности могут проводиться по следующим направлениям:

1) “Комплексный анализ информационных систем (ИС) компании и подсистемы информационной безопасности на правовом, методологическом, организационно–управленческом, технологическом и техническом уровнях. Анализ рисков”.
2) “Разработка комплексных рекомендаций по методологическому, организационно–управленческому, технологическому, общетехническому и программно–аппаратному обеспечению режима ИС компании”.
3) “Организационно–технологический анализ ИС компании”.
4) “Экспертиза решений и проектов”.
5) “Работы по анализу документооборота и поставке типовых комплектов организационно–распорядительной документации”.
6) “Работы, поддерживающие практическую реализацию плана защиты”.
7) “Повышение квалификации и переподготовка специалистов”.

Исследование и оценка состояния информационной безопасности ИС и подсистемы информационной безопасности компании предполагают проведение их оценки на соответствие типовым требованиям руководящих документов, типовым требованиям международных стандартов ISO и соответствующим требованиям компании–заказчика. К первой области также относятся работы, проводимые на основе анализа рисков, инструментальные исследования (исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей, исследование защищенности точек доступа в Internet). Данный комплекс работ также включает в себя и анализ документооборота, который, в свою очередь, можно выделить и как самостоятельное направление.

Рекомендации могут касаться общих основополагающих вопросов обеспечения безопасности информации (разработка концепции информационной безопасности, разработка корпоративной политики охраны информации на организационно–управленческом, правовом, технологическом и техническом уровнях), применимых во многих компаниях. Также рекомендации могут быть вполне конкретными и относится к деятельности одной единственной компании (план защиты информации, дополнительные работы по анализу и созданию методологического, организационно–

управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности компании).

Организационно–технологический анализ ИС компании в основном предполагает проведение оценки соответствия типовым требованиям руководящих документов к системе информационной безопасности компании в области организационно–технологических норм и анализ документооборота компании категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации.

Правильная экспертиза решений и проектов играет важную роль в обеспечении функционирования всей системы информационной безопасности и должна соответствовать требованиям по обеспечению информационной безопасности экспертно–документальным методом. Экспертиза проектов подсистем – требованиям по безопасности экспертно–документальным методом.

Работы по анализу документооборота и поставке типовых комплектов организационно–распорядительной документации, как правило, включают два направления:

– анализ документооборота компании категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации;

– поставку комплекта типовой организационно–распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно–управленческом и правовом уровне.

1.1.2 Методика построения корпоративной системы защиты информации

Главная цель любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца, защита информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, обеспечении нормальной производственной деятельности всех подразделений объекта. Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности, имущественных прав и интересов клиентов**.**

Для этого необходимо:

– отнести информацию к категории ограниченного доступа (служебной тайне);

– прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению

финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

– создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

– создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

– создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

При выполнении работ можно использовать следующую модель построения корпоративной системы защиты информации, основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799) (Рисунок 1.1).

Рисунок 1.1 – Модель построения корпоративной системы защиты информации

Представленная модель защиты информации – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

– угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

– уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

– риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика проведения аналитических работ позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого–либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

1.1.3 Методика реорганизации корпоративной системы информационной безопасности

На данный момент многие организации имеют старую корпоративную систему информационной безопасности и целесообразно рассмотреть методику ее реорганизации.

Главной целью любой системы обеспечения информационной безопасности является обеспечение устойчивого функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной торговой и производственной деятельности всех подразделений предприятия. Еще одной целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Для достижения названных целей необходимо решить следующие основные задачи:

– отнесение информации к категории ограниченного доступа (служебной или коммерческой тайне);

– прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению их нормального функционирования и развития;

– создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

– создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности.

При выполнении практических работ по реорганизации системы безопасности может быть принята следующая модель построения системы информационной безопасности, основанная на адаптации "Общих критериев" ISO 15408 и проведении анализа информационных рисков (Рисунок 1.2).

Рисунок 1.2 – Алгоритм оценивания рисков

Представленная модель – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Здесь рассматриваются следующие объективные факторы:

угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы информационной безопасности организации предлагается первоначально провести анализ информационных рисков. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

1.2 Концепция безопасности объекта информации

Концепция безопасности коммерческого банка представляет собой научно обоснованную систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты банковского дела от противоправных действий и недобросовестной конкуренции.

Под безопасностью коммерческого банка понимается состояние защищенности интересов владельцев, руководства и клиентов банка, материальных ценностей и информационных ресурсов от внутренних и внешних угроз.

Обеспечение безопасности является неотъемлемой составной частью деятельности коммерческого банка. Состояние защищенности представляет собой умение и способность кредитной организации надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам банка.

Объектами безопасности являются:

– персонал (руководство, ответственные исполнители, сотрудники);

– финансовые средства, материальные ценности, новейшие технологии;

– информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, предоставленная в виде документов и массивов независимо от формы и вида их представления).

Субъектами правоотношений при решении проблемы безопасности являются:

– Центральный банк, осуществляющий денежно–кредитную политику страны;

– коммерческий банк как юридическое лицо, являющееся собственником финансовых, а также информационных ресурсов, составляющих служебную, коммерческую и банковскую тайну;

– другие юридические и физические лица, в том числе партнеры и клиенты по финансовым отношениям, задействованные в процессе функционирования коммерческого банка как внутри страны, так и во внешне финансовых связях (органы государственной власти, исполнительные органы, организации, привлекаемые для оказания услуг в области безопасности, обслуживающий персонал, клиенты и др.);

– службы безопасности коммерческих банков и частные охранно–детективные структуры.

Концепция определяет цели и задачи системы безопасности, принципы ее организации, функционирования и правовые основы, виды угроз безопасности и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая правовую, организационную и инженерно–техническую защиту.

1.2.1 Цели и задачи системы безопасности

Главной целью системы безопасности является обеспечение устойчивого функционирования банка и предотвращение угроз его безопасности, защита законных интересов кредитной организации от противоправных посягательств, охрана жизни и здоровья персонала, недопущения хищения финансовых и материально–технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

Другими целями концепции являются:

– формирование целостного представления о системе безопасности банка и взаимоувязка различных элементов этой системы, определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объектов;

– повышение имиджа банка и роста прибыли за счет обеспечения высокого качества предоставляемых услуг и гарантий безопасности, имущественных прав и интересов клиентов.

Задачами системы безопасности являются:

– прогнозирование и своевременное выявление, и устранение угроз безопасности персоналу и ресурсам банка; причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;

– отнесение информации к категории ограниченного доступа (государственной, служебной, банковской и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов – к различным уровням уязвимости (опасности) и подлежащих сохранению;

– создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании банка;

– эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно–технических мер и средств обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерным действиям физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей банка.

1.2.2 Принципы организации и функционирования системы безопасности

Организация и функционирование системы безопасности должны соответствовать следующим принципам:

1 Комплексность:

– обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;

– обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки и использования, во всех режимах функционирования;

– способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования банка.

Комплексность достигается:

– обеспечением соответствующего режима и охраны;

– организацией специального делопроизводства с ориентацией на защиту коммерческих секретов и банковской тайны;

– мероприятиями по подбору и расстановке кадров;

– широким использованием технических средств безопасности и защиты информации;

– развернутой информационно–аналитической и детективной деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно–технических мероприятий.

2 Своевременность – упреждающий характер мер обеспечения безопасности.

Своевременность предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирование финансовой обстановки, угроз безопасности банка, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3 Непрерывность – считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

4 Активность. Защищать интересы банка необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

5 Законность. Предполагает разработку системы безопасности на основе законодательства в области банковской деятельности, информатизации и защиты информации, частной охранной деятельности и других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6 Обоснованность. Используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7 Экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность – стоимость"). Во всех случаях стоимость системы безопасности должна быть меньше размера возможного ущерба от любых видов риска.

8 Специализация. Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности банка, его функциональных и обслуживающих подразделений.

9 Взаимодействие и координация. Означает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также сотрудничества с заинтересованными объединениями и взаимодействия с органами государственного управления и правоохранительными органами.

10 Совершенствование. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно–технических требований, достигнутого отечественного и зарубежного опыта.

11 Централизация управления. Предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы безопасности.

1.2.3 Объекты защиты

К объектам, подлежащим защите от потенциальных угроз и противоправных посягательств, относятся:

– персонал банка (руководящие работники, производственный персонал, имеющий непосредственный доступ к финансам, валюте, ценностям, хранилищам, осведомленные в сведениях, составляющих банковскую и коммерческую тайну, работники внешнеэкономических служб и другие;

– финансовые средства, валюта, драгоценности;

– информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;

– средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радио– и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

– материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

– технические средства и системы охраны и защиты материальных и информационных ресурсов.

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную потенциальную уязвимость с точки зрения возможного материального или морального ущерба. Исходя из этого, они должны быть, классифицированы по уровням уязвимости, степени риска.

Наибольшую уязвимость представляют финансовые и валютные средства, особенно в процессе транспортировки, информационные ресурсы и некоторые категории персонала.

1.2.4 Основные виды угроз интересам коммерческого банка

Определение и прогнозирование возможных угроз, и осознание их опасности необходимы для обоснования, выбора и реализации защитных мероприятий, адекватных угрозам интересам банка.

В процессе выявления, анализа и прогнозирования потенциальных угроз интересам банка в рамках концепции учитываются объективно существующие внешние и внутренние условия, влияющие на их опасность. Таковыми являются:

– нестабильная политическая, социально–экономическая обстановка и обострение криминогенной ситуации;

– невыполнение законодательных актов, правовой нигилизм, отсутствие ряда законов по жизненно важным вопросам;

– снижение моральной, психологической и производственной ответственности граждан.

К угрозам безопасности личности относятся:

– похищения и угрозы похищения сотрудников, членов их семей и близких родственников;

– убийства, сопровождаемые насилием, издевательствами и пытками;

– психологический террор, угрозы, запугивание, шантаж, вымогательство;

– нападение с целью завладения денежными средствами, ценностями и документами.

1.2.5 Техническое обеспечение безопасности банка

Техническое обеспечение безопасности должно базироваться на:

– системе стандартизации и унификации;

– системе лицензирования деятельности;

– системах сертификации средств защиты;

– системе сертификации ТС и ПС объектов информатизации;

– системе аттестации защищенных объектов информатизацией.

Основными составляющими обеспечения безопасности ресурсов КБ являются:

– система физической защиты (безопасности) материальных объектов и финансовых ресурсов;

– система безопасности информационных ресурсов.

Система физической защиты (безопасности) материальных объектов и финансовых ресурсов должна предусматривать:

– систему инженерно–технических и организационных мер охраны;

– систему регулирования доступа;

– систему мер (режима) сохранности и контроль вероятных каналов утечки информации;

– систему мер возврата материальных ценностей (или компенсации).

Система охранных мер должна предусматривать:

– многорубежность построения охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;

– комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

– надежную инженерно–техническую защиту вероятных путей несанкционированного вторжения в охраняемые пределы;

– устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;

– высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию нарушителям;

– самоохрану персонала.

1.2.6 Принципы и направления взаимодействия между объектом и правоохранительными органами в области безопасности

Какой бы совершенной ни была самоорганизация безопасности коммерческого банка, она не обеспечит предотвращение преступных посягательств без взаимодействия кредитного учреждения с соответствующими правоохранительными органами и, прежде всего полицией.

Организационно–правовой основой такого взаимодействия являются: конституционные принципы равенства защиты всех форм собственности.

Целями сотрудничества являются: предупреждение и раскрытие преступных посягательств на персонал коммерческих банков, денежные средства и ценности.

Приоритетными направлениями взаимодействия банка и территориального органа внутренних дел должны быть:

Обмен информацией:

– о фактах (способах) совершения хищений денежных средств в коммерческих банках с использованием подложных банковских документов, кредитных карточек, подделки иных документов;

– о физических лицах, работающих в коммерческих банках, вкладчиках и других клиентах, подозреваемых в совершении правонарушений;

– о юридических лицах, являющихся клиентами банка, совершающих банковские операции, имеющие подозрительный характер, в целом о банковских операциях, вызывающих обоснованные сомнения в целесообразности их проведения.

Разработка совместных мер:

– противодействия предполагаемым (реальным) фактам общеуголовных проявлений в банковской системе, угрозам убийства, либо нанесения тяжких телесных повреждений, уничтожения имущества коммерческих банков, их руководителей, сотрудников и членов их семей;

– по технической укрупнённости и оборудованию средствами сигнализации объектов банка;

– по созданию так называемой "горячей линии" между банковским и территориальным органом внутренних дел (полицией);

– участия в формировании централизованного, регионального банка данных о предприятиях различных форм собственности, недобросовестных участниках кредитно–денежных отношений.

Работа по подбору, расстановке и профессиональная подготовка кадров служб банковской безопасности:

– осуществление совместной проверки кандидатур на работу в службу банковской безопасности с использованием информационных возможностей органов внутренних дел, сведений о судимости и т.д.;

– проведение совместной разработки и введение правил об ответственности персонала коммерческих банков за противоправное использование;

– использование помощи милиции в обучении и повышении квалификации кадров службы безопасности банка.

Таким образом, данная концепция позволяет руководителю коммерческого банка определить основы организации безопасности кредитного учреждения с учетом местных условий и своих возможностей по затратам и ресурсам ее обеспечения.

1.3 Обследование объекта защиты

Объектом выступает здание Алматинского филиала акционерного коммерческого банка «БАНК». Объект расположен в жилом массиве, по адресу ул. Толе би, д. 130Б.

Здание банка является двухэтажным строением. Все здание выполнено из монолитно бетонных конструкций. Крыша объекта покрыта черепицей.

В окружении имеются предприятия массового отдыха и торговые предприятия.

С севера проходит улица Жумалиева, с юга – детская площадка, прилегающая к 5–ти этажному дому, с востока – на расстоянии порядка 10 м расположен 5–ти этажный дом, с запада – 5–ти этажный жилой дом, рядом с которым находится объект.

Общая площадь территории объекта составляет 589,39 м², а длина периметра – 68,81 м. Территория объекта в темное время суток освещается.

Здание двухэтажное, длина – 21,4 м, ширина – 24,2 м. На втором этаже, над центральным входом находится балкон.

Имеется подвал. Вход в подвал расположен под лестничной клеткой.

Изменение температур в течение года в диапазоне от минус 40°С до плюс 40°С. Затоплений паводковыми водами не наблюдается. Возможно избыточное обводнение в результате действия атмосферных осадков (дождь и тающий снег). Преимущественное направление ветров – западное. Максимальная скорость ветра (без учета ураганных ветров) до 20 м/с. Максимальная высота травяного покрова на территории объекта до 0,2 м. Максимальная высота снежного покрова до 0,5 м. В весеннее и осеннее время возможны густые туманы. Предельная дальность видимости в тумане составляет 20 – 30 м. Относительная влажность воздуха до 98% при температуре 25 – 30°С.

Объект имеет обособленную территорию без ограждения периметра. На территории выделено место для стоянки автомобилей, расположенное перед фасадом здания и рассчитанного на 2–4 автомобиля.

Режим работы объекта – одна смена, время работы с 8 до 18 часов; суббота, воскресенье – выходные.

Кадровый состав банка – пятьдесят сотрудников. Организационная структура включает в себя отделы:

- управление;
- отдел бухгалтерского учета и отчетности;
- отдел по работе с клиентами;
- отдел платежных систем;
- отдел кредитных операций;
- отдел информационных технологий;
- юридический отдел;
- отдел анализа и прогнозирования;
- служба безопасности;
- отдел кадров;
- касса;
- обменный пункт;
- архивариус;
- административно–хозяйственный отдел;
- инкассация (внешняя).

Служба безопасности состоит из двух сотрудников. Охрана объекта и пропускной режим осуществляется четырьмя сотрудниками Вневедомственной охраны при МВД, обеспечивающими охрану хранилища ценностей и соблюдение режима. Охрана объекта ведется круглосуточно. В рабочее время – два поста охраны, в нерабочее – один. Посты охраны расположены на КПП, у лестничной клетки в правой части здании, на первом этаже и на входе в кассовый узел, рядом с хранилищем. Охрана оснащена рациями.

Кассовый узел выполнен в соответствии со всеми требованиями к защите.

Степень конфиденциальности информации – коммерческая, банковская тайна, персонифицированные данные.

ЛВС – с применением программных и программно–аппаратных средств защиты, средств криптографической защиты. Доступ к ЛВС основан на разделении прав пользователей. Имеется выход во внутреннюю сеть для связи с головным банком и центральным банком.

Внутренняя АТС с выходом на городскую АТС с разграничением права выхода на междугороднюю связь.

Здание находится в хорошем состоянии, трещин и разрушений конструкций не имеется. На торце здания имеется пожарная лестница, ведущая на крышу. Толщина внешних стен здания – 0,6 м, внутренних несущих – 0,4 м, стеновых перегородок – 0,2 м. Материал стен – декоративный кирпич. Все окна с двойным стеклом, рамы стоят плотно, присутствуют решетки на окнах.

Внутренние двери деревянные, с обычным замком. Имеется одна лестничная клетка, в правой части здания.

Запасной выход организован с задней стороны здания.

Хранилище ценностей относительно центрального входа расположено в левой части здания на первом этаже, вход в хранилище осуществляется через предкладовую. Вход в пред кладовую в рабочее время контролируется одним из охранников – второй пост охраны.

Руководство банка, бухгалтерия и касса расположены в левой части здания на втором этаже.

1.3.1 Класс защиты объекта информатизации

В качестве исходных данных для определения необходимых мер по укреплению объекта информатизации инженерными средствами защиты и разработки качественной системы физической охраны необходимо произвести классификацию объекта информатизации в соответствии с «Требованиями и нормами проектирования по защите объектов от преступных посягательств»

Выбираемая группа защиты от взлома строительных конструкций должна соответствовать стоимости и значимости для потенциальных преступников имущества (ценностей), которое находится в помещениях объекта. Кроме этого, необходимо учитывать месторасположение объекта и доступность проникновения в помещения объекта, причем таким образом, что более высокие требования должны предъявляться к местам, где злоумышленник может действовать в относительной безопасности.

В зависимости от значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей, размещенных на объекте, последствий от возможных преступных посягательств на них, все объекты, их помещения и территории подразделяются на две группы (категории): А и Б. Объекты подгрупп АI и АII – это объекты особо важные, повышенной опасности и жизнеобеспечения, противоправные действия (кража, грабеж, разбой, терроризм и другие) утрата которых может привести к крупному.

Объекты подгрупп БI и БII – это объекты, хищения которых может привести к ущербу в размере до 500 минимальных размеров оплаты труда и свыше 500 соответственно.

Объекты кредитно–финансовой системы (банки, операционные кассы вне кассового узла, дополнительные офисы, пункты обмена валюты, банкоматы) относятся к объектам группы АI.

Схема помещений 1 и 2 этажей будет представлена в приложении А.

1.3.2 Категорирование помещений

Категорирование помещений производится по виду и концентрации в них материальных ценностей. Помещениям присваиваются соответствующие категории, которые описаны в таблице 1.1.

Таблица 1.1 – Категории помещений

Категория	Производственное или другое назначение объекта (помещения)	Характеристика значимости ценностей
1	Объекты (помещения) с постоянным хранением: – огнестрельного оружия и боеприпасов; – наркотических и ядовитых веществ; – драгоценных металлов и камней, ювелирных изделий, ценных предметов старины, искусства и культуры; крупных денежных средств, валюты и ценных бумаг; – секретной документации и других особо ценных и особо важных товарно–материальных ценностей.	Товары, предметы и изделия особой ценности и важности, утрата которых может принести особо крупный или невосполнимый материальный и финансовый ущерб, создать угрозу здоровью и жизни большого количества людей, находящихся на объекте и вне его, привести к другим тяжелым последствиям
2	Объекты (помещения) с постоянным хранением: – табельного огнестрельного оружия и боеприпасов (комнаты оружия); – радиоизотопных веществ и препаратов; – ювелирных изделий, предметов старины, искусства и культуры; – денежных средств, валюты и ценных бумаг (главные кассы объектов). Спец архивы и спец библиотеки.	Ценные и важные товары, предметы и изделия, утрата которых может принести значительный материальный и финансовый ущерб, создать угрозу здоровью и жизни людей, находящихся на объекте
3	Объекты (помещения) с постоянным или временным хранением: – промышленных товаров и продуктов питания; – аудио–, видео–, орг–, и телетехники; Служебные, конторские помещения и т.п.	Товары, предметы и изделия повседневного спроса и использования
4	Объекты (помещения) с постоянным или временным хранением: – технологического и хозяйственного оборудования; – технической и конструкторской документацией; – инвентарь; Подсобные и вспомогательные помещения и т.п.	Товары, предметы и изделия технологического и хозяйственного назначения

Исходя из выше описанного, на данном объекте выделены помещения следующих категорий:

первой категории – хранилище ценностей;

второй категории – касса;

третьей категории – все остальные помещения, кроме подсобного;

четвертой категории – подсобное помещение.

1.3.3 Результат анализа характеристики объекта

Охрана объекта обеспечивается силами дежурящего вахтера (сотрудника Вневедомственной охраны МВД) и двумя вооруженными охранниками (также сотрудники Вневедомственной охраны МВД), что не обеспечивает высокий уровень безопасности объекта. Сотрудники охраны в основном обеспечены всем необходимым для выполнения поставленных задач. Вместе с тем, отсутствие на КПП, и на объекте в целом, технических средств охраны и малый состав не позволяет постовым эффективно выполнять свои обязанности.

Для выделенных (категорированных) помещений требуется усиленный режим охраны, при выборе технических средств требуется уделить особое внимание выбору конкретных вариантов решения задачи защиты.

1.4 Модель потенциального нарушителя

Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Человек обеспечивает функционирование системы, ее охрану и защиту. Он, несомненно, является первым по значимости носителем информации. В то же время, он, при определенных обстоятельствах, может стать главным источником угрозы защищаемой информации. Поэтому рассмотрение модели нарушителя, которая отражает его практические и теоретические возможности, априорные знания, время и место действия, несомненно, имеет практическую значимость.

Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной системы.

При разработке модели нарушителя определяются:

– предположения о категориях лиц, к которым может принадлежать нарушитель;

– предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

– предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

– ограничения и предположения о характере возможных действий нарушителей.

1.4.1 Основные характеристики нарушителей

Для любого объекта можно выделить классы нарушителей, действия которых наиболее вероятны для данного объекта. Для каждого класса нарушителей характерны свои способы действий, цели, задачи и т.п., а соответственно, методы противодействия.

Выделим несколько основных характеристик, которые позволят описать основные группы нарушителей:

– мотивы;
– цели;
– финансовое обеспечение;
– наличие и уровень профессиональной подготовки нарушителей;
– техническое обеспечение;
– наличие и качество предварительной подготовки преступления;
– наличие и уровень внедрения нарушителей на объект.

Мотивы деятельности нарушителей:

– желание приобрести материальные ценности (в т.ч. деньги);
– конкурентная борьба;
– сведение личных счетов;
– политические мотивы;
– религиозные мотивы;
– любопытство;
– ошибка;
– неосознанные, немотивированные действия под влиянием алкоголя, или других наркотических веществ.

Цели нарушителей при совершении конкретных преступлений:

– кража материальных ценностей;
– кража информации;
– уничтожение материальных ценностей;
– уничтожение информации;
– создание помех функционированию объекта (вплоть до полного прекращения функционирования объекта);
– ухудшение условий жизнедеятельности людей;
– физическое уничтожение людей.

Перечисленные здесь цели можно, также, назвать "Основными методами совершения противоправных действий". Перечисленные цели являются общими.

Финансовое обеспечение

Финансовое обеспечение деятельности нарушителей может изменяться в самых широких пределах. Поэтому, в общем случае, выделим 3 уровня финансового обеспечения:

– практически не ограниченное;
– ограниченное;
– отсутствует.

Наличие и уровень профессиональной подготовки нарушителей

Наличие и уровень профессиональной подготовки нарушителей зависит от финансового обеспечения, но не связан с ним напрямую. Понятно, что организации, обладающей достаточным финансовым обеспечением, проще найти профессионалов в любой области.

Однако хороший уровень профессиональной подготовки может быть, например, у небольшой группы выходцев из какой–либо спецслужбы. Также, много преступлений в одиночки, хорошо подготовленные профессионально. В том числе – самоучки.

Обратный случай – попадаются криминальные группы, сумевшие получить финансирование грубыми методами, но не имеющие достаточной профессиональной подготовки. В последнее время, таких групп становится все меньше и меньше.

Техническое обеспечение

Техническое обеспечение гораздо больше связано с финансовым, нежели профессиональная подготовка. Во многих, для преодоления систем безопасности требуется дорогостоящее оборудование и материалы. В том числе: оборудование и оснастка для разрушения и других способов преодоления технических укреплений; контрольно–измерительная аппаратура, для обнаружения и идентификации технических средств; аппаратура для блокирования технических средств, вооружение. Для террористов – взрывчатые вещества и т.п.

Наличие и качество предварительной подготовки преступления

Эффективность действий нарушителя серьезно зависит от качества предварительной подготовки преступления. Подготовка преступления включает в себя целый ряд вопросов: планирование, разведка, внедрение на объект, проведение предварительной работы по блокированию технических средств и т.п.

Выделим 3 класса подготовки преступления:

1 Долговременная подготовка – наиболее эффективна для нарушителей, она позволяет провести весь комплекс подготовительных операций, вплоть до внедрения в руководящие структуры объекта. Время долговременной подготовки от нескольких недель, до нескольких лет.

2 Оперативная подготовка включает в себя в первую очередь техническую подготовку группы нарушителей. Время оперативной подготовки – от нескольких часов до нескольких недель. Чаще всего, за это время сложно обеспечить внедрение на объект, провести соответствующую разведку и техническую подготовку на объекте.

3 Отсутствие подготовки характерно для случайных преступлений, совершаемых одиночками или небольшими группами.

Наличие и уровень внедрения нарушителей на объект

Наличие и уровень внедрение нарушителей на объект, совершенно не обязательно зависят от предварительной подготовки преступления. Во многих случаях, преступления совершают сами сотрудники объектов. Причем, преступники могут занимать любые должности, вплоть до высшего руководства.

Целесообразно выделить 2 класса внедрения на объект:

Случайное внедрение – нарушители изначально работают на объекте не с целью совершения преступлений.

Целенаправленное внешнее внедрение – нарушители внедряются на объект с заранее поставленной целью – совершение преступления.

1.4.2 Классификация нарушителей (основные типы нарушителей)

На основании вышеописанных характеристик, выделим возможные типы нарушителей, применительно к защите Алматинского филиала АКБ «БАНК». Система защиты объекта должна строиться исходя из предположений о следующих типах нарушителей:

1) *"Неопытный (невнимательный) пользователь"* – сотрудник АКБ «БАНК» (или подразделения другого ведомства, имеющий доступ в помещения ограниченного доступа), который может предпринимать попытки выполнения запрещенных операций, нарушения целостности системы защиты, доступа к объектам системы защиты с превышением своих полномочий, изменением конфигурации системы защиты и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

2) *"Любитель"* – сотрудник АКБ «БАНК» (или подразделения другого ведомства, имеющий доступ в помещения ограниченного доступа), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа, недостатки в построении системы защиты и доступные ему штатные средства. Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические средства или стандартные дополнительные технические средства.

3) *"Мошенник"* – сотрудник АКБ «БАНК» (или подразделения другого ведомства, имеющий доступ в помещения ограниченного доступа), который может предпринимать попытки выполнения незаконных технологических операций, изменение конфигурации системы защиты, нарушение ее целостности и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные аппаратные и программные средства от своего имени или от имени другого сотрудника.

4) *"Внешний нарушитель (злоумышленник)"* – постороннее лицо или сотрудник АКБ «БАНК» (или подразделения другого ведомства, имеющий

доступ в помещения ограниченного доступа), действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, включая использование специальных инструментальных и технологических средств, используя имеющиеся слабости системы защиты АКБ «БАНК».

5) *"Внутренний злоумышленник"* – сотрудник подразделения АКБ «БАНК», действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками АКБ «БАНК». Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы защиты), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных и использование специальных инструментальных и технологических средств), а также комбинации воздействий как изнутри, так и извне АКБ «БАНК».

1.5 Техническое задание на разработку интегрированной системы физической охраны объекта информатизации

Основным документом, который необходимо изучить перед началом работ над ТЗ ИСБ, является "Концепция безопасности объекта". В этом документе определены задачи, которые ставятся в структуре охраны объекта перед техническими средствами охраны (ТСО), их состав, роль и место, взаимодействие с другими элементами обеспечения безопасности объекта. В нем также определена расчетная стоимость ТСО, исходя из оценки возможного ущерба от угроз, которые должны предотвратить эти ТСО. Другие исходные данные: генплан территории объекта; архитектурно–строительные чертежи зданий и сооружений; план физической охраны объекта. Для проектирования отдельных подсистем могут потребоваться частные исходные данные: схемы электропроводок, классификация помещений по пожарной и взрывопожарной опасности, характеристики строительных конструкций зданий и сооружений, планы эвакуации при пожаре, чертежи вентиляции и отопления, конструктивные чертежи фальшполов и подвесных потолков, чертежи отдельных элементов конструкций и прочее. Эти данные должны идти как приложение к ТЗ ИСБ или к ЧТЗ. Важным элементом работы является обследование объекта с целью уточнения исходных данных и его характеристик.

Разработка ТЗ ИСБ является ключевым этапом работы над созданием ИСБ объекта, т.к. от правильности и обоснованности принятых на этом этапе решений, зависит вся дальнейшая работа над системой и сможет ли она в последующем выполнять в полном объеме возложенные на нее функции.

Работа над ТЗ ИСБ требует глубоких и разносторонних знаний в различных областях, поэтому к ней должны привлекаться наиболее квалифицированные специалисты по системам безопасности и эксперты из смежных отраслей.

Включаемые в ТЗ ИСБ требования должны соответствовать современному уровню развития науки и техники. Задаваемые требования не должны ограничивать исполнителей работ в поиске и реализации наиболее эффективных технических, экономических и других решений.

1.6 Обзор технических решений по обеспечению физической безопасности

1.6.1 Выбор IP адресации

Преимущества систем на IP адресации:

1 Простота монтажа и подключения к системе видеонаблюдения.

2 Предобработка данных на стороне IP – устройства.

3 Высокое качество изображения (прогрессивная развертка, мегапиксельное разрешение, режим день /ночь).

4 Использование активного сетевого оборудования (multicast, QoS, IGMPv3).

5 Поддержка PoE–Power–over–Ethernet (IEEE 802.3af).

6 Использование открытых стандартов (SNMP,HTTP,RTP).

7 Возможность подключение периферийных устройств к IP–камерам/серверам (IO, микрофоны, громкоговорители).

8 Возможность гибкой настройки логики системы безопасности.

9 Возможность удаленного администрирования и мониторинга системы.

10 Разграничение прав доступа к системе безопасности (LDAP).

11 Отказоустойчивость.

12 Масштабируемость.

13 Простота организации и обслуживание системы.

14 Широкие возможности по интеграции со сторонними системами.

15 Преимущества решений для обеспечения физической безопасности и интеллектуального управления зданиями.

16 Преимущества сетевых решений для обеспечения физической безопасности.

Создание недорогих, модульных и лучших в своем классе систем физической безопасности, взаимодействующих с существующими системами. Решения для обеспечения физической безопасности разработаны с применением обширного опыта Cisco в области сетевых и видео технологий:

– системы видеонаблюдения, контроля доступа, координации ответных мер и оповещения;

– удобство развертывания, эксплуатации и технического обслуживания;

– тесная интеграция с IP–сетями Cisco (медиасеть);

– защита сделанных капиталовложений по мере перехода на новые технологии;

– поддержка открытых стандартов.

Использование сети как открытой масштабируемой платформы для интеграции средств безопасности дает организациям такие преимущества, как эксплуатационная гибкость, повышение надежности защиты, снижение стоимости владения и рисков.

Решение Cisco по обеспечению физической безопасности

1 Система IP–видеонаблюдения Cisco Video Surveillance Manager(VSM), с ее помощью можно осуществлять видеопотоки, организацию и введение архивов, авторизация доступа пользователей, предоставление АРМ операторов и администрирования, интеграция и автоматизация.

2 Линейки IP–камер:

– SD–камеры: Формат MPEG4,30 кадр/сек с разрешением D1(702x576),поддержка режима день/ночь ,звука. Встроенный детектор движения. Поддержка PoE.

– HD–камера: Формат H/264, 30 кадр/сек с разрешение 1080p (1920x1080), поддержка режима день/ночь, звука, I/O. Дополнительный DSP для обработки видео. Возможность установки USB карты памяти. Поддержка PoE.

3 Мультисервисные платформы.

1U–4U сервера со встроенными дисковыми массивами.

1.6.2 Пожарная сигнализация противопожарная автоматика.

Датчик дыма Cisco SC460 предназначен для установки внутри помещений. Служит для обнаружения задымления в помещении (Рисунок 1.3).

Рисунок 1.3 – Датчик дыма, влажности и температуры

При установке в помещении, в шкафу и т.п. датчик контролирует появление дыма, измеряет температуру и относительную влажность. Чувствительность к дыму данного датчика колеблется в пределах 0,05–0,2

дБ/м. Температурный диапазон составляет от минус 10 до плюс 55 градусов по Цельсию. Диапазон влажности – от 10 до 95 процентов влажности. Благодаря быстрому действию срабатывания в 10 секунд, этот датчик пользуется популярностью. Мы выбрали данный датчик, благодаря его быстродействию и точному обнаружению задымления в зоне его действия.

Датчик движения, вибрации, температуры Cisco SC470 предназначен для обнаружения посторонних лиц в зоне действия устройства (Рисунок 1.4).

Рисунок 1.4 – Датчик движения, вибрации и температуры

Датчик необходим для контроля движения в инфракрасном диапазоне, измерения температуры и обнаружения вибрации на объектах. Контролируемое расстояние до 12 метров. Макс. удаленность одиночного датчика от модуля мониторинга 200 метров. Угол зрения пассивного инфракрасного датчика 110 градусов, что обеспечивает хороший обзор входов, дверей и общественных зон с широким горизонтальным углом.

Датчик влажности Cisco SC510 предназначен для обнаружения влажности на объекте (Рисунок 1.5).

Рисунок 1.5 – Датчик влажности

Необходим для измерения относительной влажности на различных объектах. Измеряемый диапазон влажности: 10–95%. Макс. удаленность датчика от модуля 50 метров.

1.6.3 Система контроля доступа

Система контроля доступа Cisco использует IP сеть как платформу, на которой разворачиваются крупномасштабная система разграничения прав. В эту систему входит шлюз контроля доступа, серверная платформа 1RU, выдача пропусков, менеджер по управлению датчиками с отображением карт помещений, интеграция с видеонаблюдением. Система контроля доступа представлена на рисунке 1.6.

Рисунок 1.6 – Система контроля доступа.

Рассмотрим компоненты крупномасштабной системы разграничения прав:

Шлюз физического доступа Cisco

Шлюз физического доступа Cisco, является обязательным компонентом любого контроля доступа (Рисунок 1.7).

Возможность подключение замков и считываетлей по IP (поддерживается PoE), подключение до 2 дверей (Wiegand), 250 000 пользователей, 150 000 событий, шифрование AES 128бит, возможность расширения дополнительными модулями.

Рисунок 1.7 – Шлюз физического доступа Cisco

Все характеристики шлюза контроля доступа представлены в таблицах 1.2 и 1.3.

Таблица 1.2 – Характеристики шлюза физического доступа Cisco

Особенность	Описание
Управляемые двери	Возможность подключения до двух дверей.
Модуль поддержки	До 15 дополнительных модулей могут быть подключены к шлюзу физического доступа Cisco. Эти модули могут быть подключены на 3–х проводной шине контроллеров (CAN). Все модули должны быть в пределах 400 метров от шлюза физического доступа Cisco.
Блок питания	Внешние устройства, такие как считыватель или замок может питаться от шлюза физический доступ Cisco. Максимальный потребляемый ток ограничивается 650 мА при 12 В постоянного тока.
Кэш учетных данных	250000 учетных данных можно кэшировать и в зашифрованном виде.
Кэш событий	150000 события могут быть помещены в буфер.
Шифрование	Все коммуникации представлены в зашифрованном виде,128–битный Advanced Encryption Standard (AES).

Таблица 1.3 – Разъемы шлюза физического доступа Cisco

Соединитель	Описание
Ethernet	Есть два разъема 10/100 Base–TX RJ–45: • Ethernet–0: Используется для подключения шлюза физического доступа Cisco к сети. Он также может быть использован для подачи питания, по Ethernet (PoE) на устройство. • Ethernet–1: Используется для перехода на страницу конфигурации.
Выходы	Есть три релейных выхода Form C, с контактами номинальных 5А, 30В постоянного тока. Каждый из них может быть настроен либо как нормально замкнутый (NC) или нормально открытый (NO).
Power Fail Input	"Power Fail" поднимает тревогу при активации.
CAN Bus	CAN шина 3–выхода для подключения дополнительных модулей.

Модули расширения шлюза физического доступа Cisco

Модуль расширения шлюза физического доступа Cisco является дополнительным модулем, который может быть подключен к шлюзу

физического доступа Cisco, который позволяет расширить подключение и включить дополнительные шлюзы.

К модулю ввода физического доступа Cisco можно подключить до 10 шлюзов, каждый из которых может быть настроен как контролируемый или неконтролируемый. Модуль должен быть использован в сочетании со шлюзом физического доступа Cisco, и не может использоваться автономно.

Характеристики дополнительных модулей шлюза физического доступа Cisco:

– подключение по шине CAN;
– удаление до 400 метров от дверного контроллера.

Модуль считывателей (Рисунок 1.8).

Рисунок 1.8 – Модуль считывателей

Данный модуль имеет возможность подключение до 2 дверей, питание датчика производится по кабелю RJ–45, 12 вольтами постоянного тока. Так же имеется порт считывателя от пяти до десяти pin Weigand, три входа и три выхода.

Модуль цифровых входов (подключение датчиков) (Рисунок .1.9).

Рисунок 1.9 – Модуль цифровых входов

Модуль цифровых входов имеет подключение до 10 входов к шлюзу физического доступа Cisco по шине CAN. Питание датчика производится по кабелю RJ–45, 12 вольтами постоянного тока.

Модуль цифровых выходов (подключение устройств) (Рисунок 1.10).

Рисунок 1.10 – Модуль цифровых выходов

Модуль цифровых входов имеет подключение до 8 входов к шлюзу физического доступа Cisco по шине CAN. Питание датчика производится по кабелю RJ–45, 12 вольтами постоянного тока. Так же имеет 8 портов выхода.

Схема подключения дополнительных модулей развертывания к головному шлюзу физического доступа Cisco. Максимальное допустимое расстояние 400 метров (Рисунок 1.11).

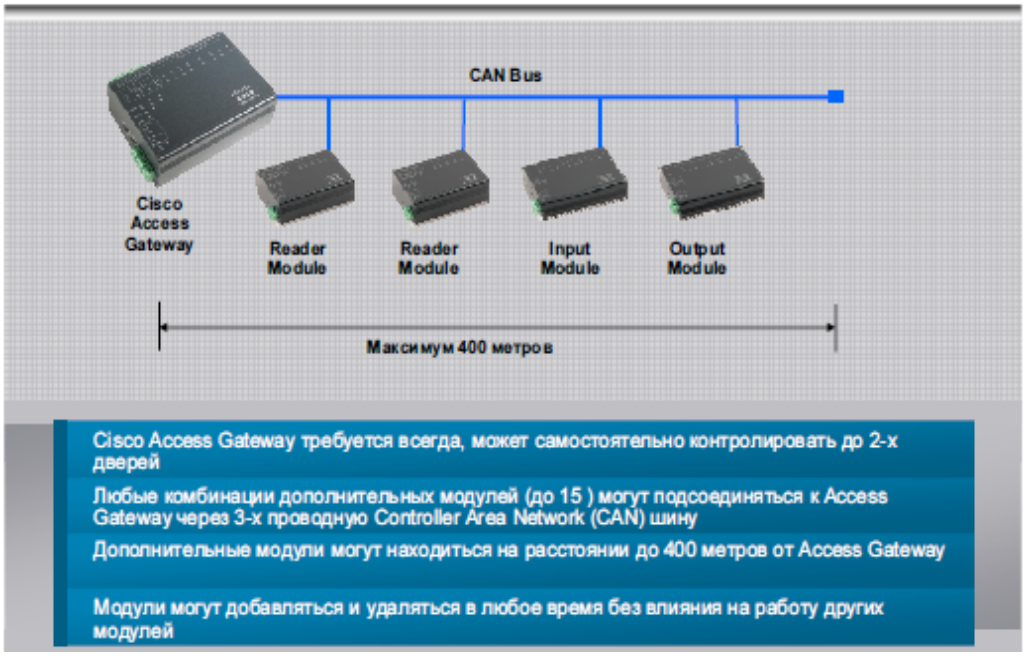


Рисунок 1.11 – Архитектура развертывания

Схема подключения к головному модулю шлюза физического доступа Cisco, дополнительных модулей. Возможность настройки всех датчиков через Cisco Physical Access Manager. Через глобальные сети WAN. Настройка маршрутизации производится посредством коммутатора (Рисунок 1.12).

Интеграция с IT–системами:

– Подсчет количества людей в здании.
– Учет активности посетителей по различным зонам.

– Интеграция с Цифровыми вывесками – вывод индивидуальной информации.

– Усиленная безопасность – активация портов коммутаторов, IP–телефонов и учетных записей.

– ERP – Отслеживание технологических процессов, фиксация доступа в наряде на работу.

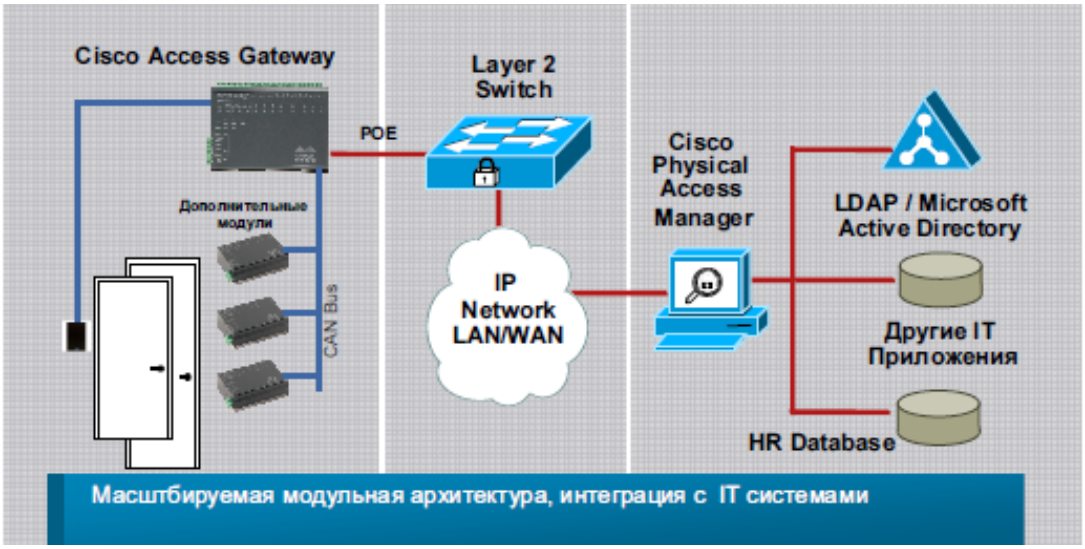


Рисунок 1.12 – Уникальная расширяемая архитектура

Система управления физическим доступом

Функции, которые выполняет Cisco Physical Access Manager:

– Настройка шлюзов и модулей, мониторинг активности, регистрация пользователей.

– Интеграция с IP–приложениями и хранилищами данных.

– Повышение уровня безопасности за счет отслеживания доступа в здание.

– Улучшение контроля над обстановкой за счет интегрированной системы управления видеонаблюдением Cisco Video Surveillance Manager.

– Интеграция на уровне обмена событиями с Cisco VSM.

– Позволяет ассоциировать камеру с дверью.

– При открытии двери создается событие на которое может быть просмотрено видео.

Cisco Physical Access Manager является приложением для управления и настройки шлюза физического доступа Cisco и модулей расширения. Cisco Physical Access Manager представлен на рисунке 1.13, используется для мониторинга активности, регистрации пользователей, а также интеграции с ИТ–приложениями и хранилищем данных.

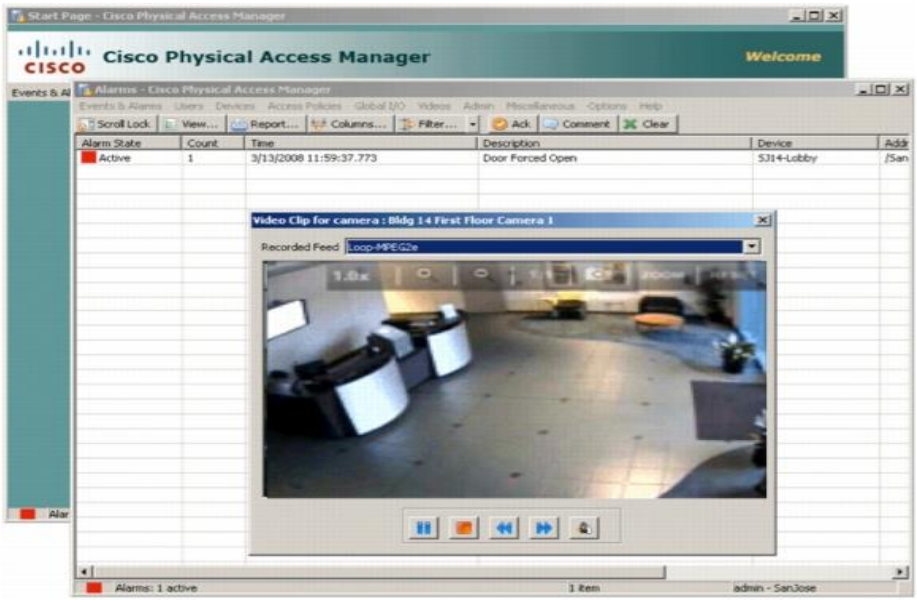


Рисунок 1.13 – Cisco Physical Access Manager

При входе в помещение видеокамера сравнивает данные с базой имеющихся сотрудников в ней. И просматривает журнал посещений. Если в базе не зарегистрирован человек, который проник в помещение, то сигнал идет на пульт мониторинга (Рисунок 1.14).

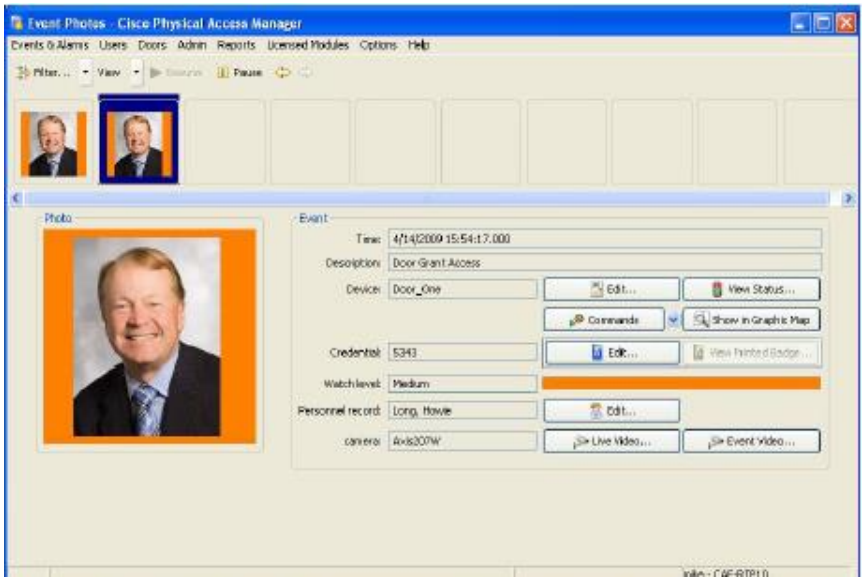


Рисунок 1.14 – Сверка с фотографией

При посещении любой из охраняемых зон идет видеонаблюдение. При входе в помещение идет сравнение с базой имеющихся сотрудников по фотографии. Это помогает оградить злоумышленника от секретных данных (Рисунок 1.15).

Рисунок 1.15 – Мониторинг

Cisco Physical Access Manager

Бывает двух форм–факторов – аппаратное устройство (Рисунок 1.16) и виртуальное устройство для Cisco Unified Computing System (Cisco UCS) B и серии C (Рисунок 1.17).

Рисунок 1.16 – Cisco физическая безопасность MULTISERVICES Платформа 1–RU

Рисунок 1.17 – Virtual Appliance для Cisco Unified Computing System (UCS) B и C Series

У Cisco Physical Access Manager имеются свои особенности:

– Microsoft Active Directory – Администрирование пользователей Менеджера шлюза физического доступа Cisco, могут быть настроены на использование Microsoft Active Directory для аутентификации.

– Хранение данных дополнительный лицензируемый модуль позволяет создавать шаблоны фотографий пользователей и регистрацию пользователей в базе данных.

– Политики доступа области, в которые допущены пользователи, могут быть назначены и записаны в записи, основанные на графиках.

– Управление учетными данными учетные данные владельца карточки можно редактировать.

– Сигнализации и управления событиями – Cisco Access Gateway Manager, обеспечивает представление событий и тревог в системе.

На рисунке 1.18 представлены основные характеристики мультисервисной платформы 1RU.

– Захват видео 8 и 16 портовые карты До 16 портов на 1RU, 48 портов на 2RU.

– Гибкий выбор вариантов кодирования H.264, dual streams, 30 и 15 кадр/сек, D1 и CIF Motion JPEG, dual streams, 15 и 10 кадр/сек, D1 and CIF.

– Функции Кодирование видео на аппаратных DSP процессорах, управление до 32 поворотных камер через последовательный интерфейс и встроенный визуальный детектор.

Рисунок 1.18 – Основные характеристики платформы 1RU

1.6.4 Системы Телевизионного видеонаблюдения

Система телевизионного видеонаблюдения Cisco использует IP сеть как платформу, на которой разворачиваются крупномасштабная система захвата

видео. В эту систему входят IP камеры, мультисервисная платформа 1RU, медиа сервер, менеджер операций по обработке видео, виртуальная матрица. Система телевизионного видеонаблюдения Cisco представлена на рисунке 1.19.

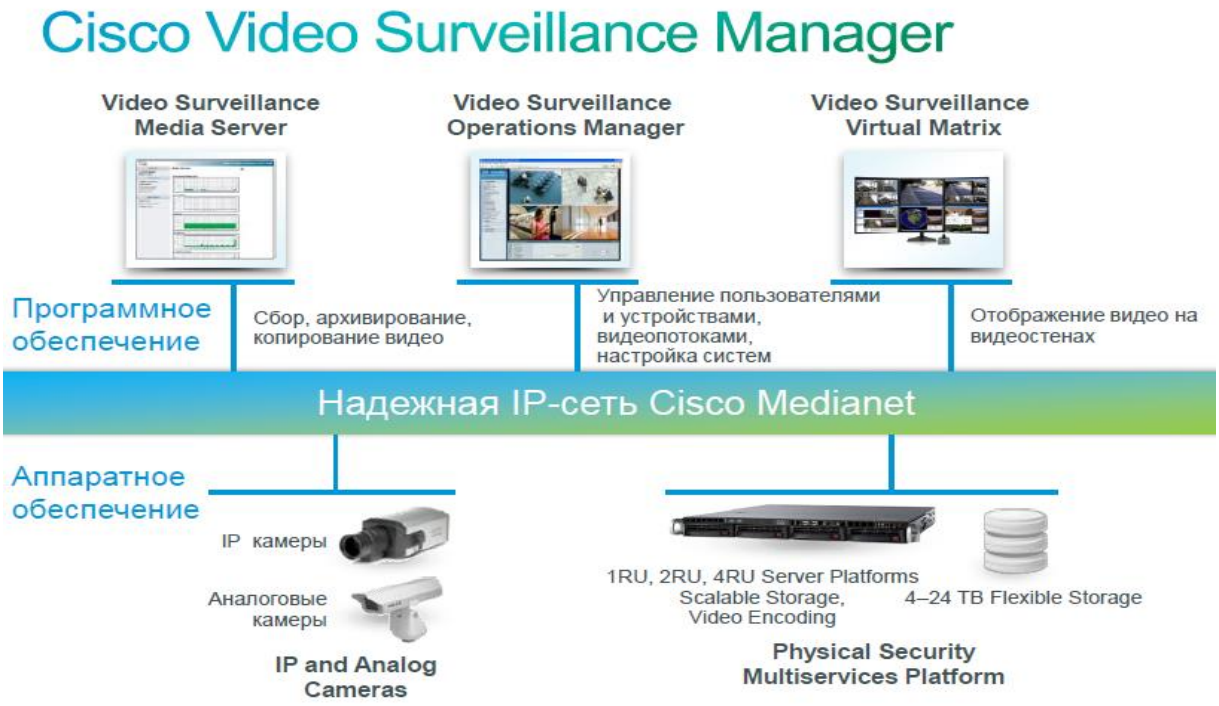


Рисунок 1.19 – Система телевизионного видеонаблюдения.

Рассмотрим компоненты система телевизионного видеонаблюдения.

Уличная сетевая беспроводная видеокамера Cisco 2500W

Сетевая беспроводная видеокамера Cisco 2500W входит в состав серии Cisco 2500 и может быть установлена на объектах, где затруднительно применение стандартного проводного подключения. Она имеет 1/3" КМОП–матрицу с WDR и прогрессивной разверткой, и способна автоматически переключаться из дневного в ночной режим видеонаблюдения и обратно при освещенности 0,4 лк. При этом беспроводная видеокамера может передавать по IP–сети видеопотоки в MPEG–4 с разрешением до D1 (720x576 пикс.) при 25 к/с, функционируя в соответствии с IEEE 802.11 b/g и технологиями защиты данных WEP, WPA–PSK/WPA2. Cisco 2500W поддерживает двунаправленное аудио–, видео–сопровождение и может быть настроена через веб–браузер или ПО CVSM. Она помещена в алюминиевый корпус, получает питание по технологии PoE либо от адаптера 12 VDC и может работать внутри/вне помещения.

В отличие от проводной видеокамеры той же серии, Cisco 2500W предусматривает возможность беспроводной трансляции данных IP–видеонаблюдения. Ее легко установить на объекте в пределах досягаемости приемо–передатчика при помощи обычного кронштейна либо опциональной

поворотной/наклонной платформы. Алюминиевый корпус Cisco 2500W позволяет ей работать в помещениях в диапазоне температур от 0° до +50°С либо на улице, при установке в термокожух с обогревателем и вентилятором (Рисунок 1.20).

Рисунок 1.20 – Сетевая беспроводная видеокамера Cisco 2500W.

Эта беспроводная видеокамера подходит для круглосуточного видеонаблюдения, в том числе, в меняющихся условиях освещенности, поскольку она оборудована автоматическим ИК–фильтром и имеет чувствительность в цветном режиме 0,4 лк, а в черно–белом – 0,04 лк.

Современный беспроводной интерфейс Cisco 2500W для сетевого подключения

Организация IP–системы видеонаблюдения на объекте, где развернута локальная беспроводная сеть, с применением Cisco 2500W заметно упрощается, поскольку эти видеокамеры имеют 2 антенны, поддерживают 1x2 Multiple Input Multiple Output (MIMO), повышающую производительность и дальность связи, используют стандарт IEEE 802.11b и более современный IEEE 802.11g. Оба стандарта предусматривают использование диапазона частот 2,4 ГГц, но при трансляции видео– и аудиоданных, которые беспроводная видеокамера передает через интерфейс wi–fi приемо–передатчика точки доступа, с применением 802.11g скорость будет 54 Мбит/с против 11 Мбит/с у 802.11b. Кроме того, Cisco 2500W поддерживает и проводное подключение к сети Ethernet 10/100BASE–TX, удобное, например, для ее первоначальной настройки.

Надежное шифрование и защита видеоданных при беспроводном соединении

Чтобы обезопасить передаваемые с видеокамеры Cisco 2500W данные видеонаблюдения от несанкционированного доступа, перехвата или фальсификации, применяются разные алгоритмы шифрования и механизмы защиты информации, в частности, поддерживаются сетевые протоколы аутентификации 802.1x. Для защиты соединения в пределах LAN Cisco 2500W задействует WEP (64/128–битный уровень), а для надежной фильтрации

доступа беспроводная видеокамера применяет WPA–PSK/WPA2 (Wi–fi Protected Access Preshared Key) в версиях персонального и корпоративного доступа (Enterprise). Помимо этого, функционируют и стандартные методы защиты данных, такие как фильтрация IP–адресов, система паролей и др.

Сетевые возможности и сервисы Cisco 2500W

Функционирование видеокамеры в проводной/беспроводной сети передачи данных обеспечивается за счет поддержки различных сетевых протоколов, среди которых DHCP, FTP, HTTP, TCP/IP, SNMP, SSL/TLS. Так, для надежной и безопасной идентификации Cisco 2500W в IP–сети применяется Cisco Discovery Protocol (CDP). С помощью сервиса Quality of Service (QoS) гибко настраиваются параметры видеопотоков, которые транслирует беспроводная видеокамера, для оптимального распределения трафика, то есть для гарантированной передачи приоритетных потоков без потери пакетов. Вместе с тем, для эффективного управления полосой пропускания поддерживается режим Multicast.

Купольная IP камера для размещения в помещениях

Cisco Video Surveillance 5010 и 5011. Крытая фиксированная купольная IP HD Камера. Она предназначена для установки внутри помещений. Быстрая и легкая установка. В 5010 и 5011 камеры обеспечивают высокую четкость благодаря (HD) разрешению. Она имеет 1/3" КМОП–матрицу с WDR и прогрессивной разверткой, и способна автоматически переключаться из дневного в ночной режим видеонаблюдения и обратно при освещенности 0,4 лк. При этом беспроводная видеокамера может передавать по IP–сети видеопотоки в MPEG–4 с разрешением до D1 (720x576 пикс.) при 25 к/с, функционируя в соответствии с IEEE 802.11 b/g (Рисунок 1.21).

Рисунок 1.21 – Фиксированная купольная камера

Камеры включают 2,8–8–мм варифокальный мегапиксельный объектив. Готовый к установке в помещении. Все модели также включают в себя расширенные низкой освещенности технологии и механический ИК–фильтр для повышенной чувствительности в условиях низкой освещенности. Доступны дополнительные линзы. В 5010 и 5011 камеры поддерживают два одновременных видеопотоков, которые могут быть сжатые в MJPEG и

форматов H.264 через несколько конфигураций разрешения. Камеры могут записывать видео в реальном времени (30 кадров в секунду [IPS]) с разрешением Full HD с использованием сжатия H.264 для оптимизации пропускной способности и эффективности хранения. Потоки могут быть сконфигурированы в различных частотах, скорости передачи, и группы изображений (GOP) Профили для дополнительного администрирования полосы пропускания.

Камеры просты в установке. Функция автоматического управление фокусом делает резкое изменение картинки благодаря изменению фокуса камеры. Удобное видео–гнездо установки исключает необходимость использовать ноутбук для просмотра видео при установке камеры.

1.6.5 Менеджер управления системой телевизионного видеонаблюдения

Cisco Video Manager

Cisco Video Manager видеонаблюдения для Cisco Unified Computing System Express (UCS Express) представляет собой систему для подключения линейки продуктов видеонаблюдения Cisco.

Многофункциональное ПО Cisco Video Surveillance Manager (CVSM) разработано для системы IP–видеонаблюдения распределенных объектов. Программное обеспечение CVSM инсталлируется на подключенный к сети компьютер или на специализированный аппаратный компонент системы видеонаблюдения – Encoding Server. Это ПО имеет архитектуру «клиент–сервер», поддерживает форматы сжатия H.264, MPEG–4 и M–JPEG, и позволяет конфигурировать IP–камеры видеонаблюдения, роутеры, видеосерверы Cisco , в составе локальной или распределенной системы видеонаблюдения. Video Surveillance Manager имеет два базовых модуля: Media Server для обработки, записи, хранения аудио– и видеоинформации, управления видеопотоками, и Operations Manager, позволяющий удаленно конфигурировать IP–камеры и видеосерверы. Кроме того, модуль Virtual Matrix выполняет функции виртуального матричного коммутатора и обеспечивает вывод «живого» или архивного видео на мониторы или видеостены систем видеонаблюдения и безопасности.

Сетевые камеры Cisco обеспечивают:

Отличное качество видео даже в сложных условиях освещенности.

1 Две ветки:

– камеры стандартного разрешения (SD);

– камеры высокого разрешения (HD) (1080p), выделенный DSP для задач обработки видео на камере.

2 Широкий динамический диапазон.

3 Гибкие настройки:

– аутентификация, фильтрация ip адресов;

– настройка потока вещания: QoS, multicast, управление битрейтом.

Сравнение качества съемка камер Cisco с камерами других поставщиков (Рисунок 1.22).

Рисунок 1.22 – Проработка деталей изображения в сложных условиях освещенности

Сравнение камер Cisco с другими камерами при сложной световой обстановке (Рисунок 1.23).

Рисунок 1.23 – Нет засветки камеры при встречном солнечном свете

Камеры поддерживают режим день – ночь. Что помогает для наблюдения и в дневное и в ночное время (Рисунок 1.24).

Рисунок 1.24 – Режим работы «день/ночь»

Сравнение систем видеонаблюдения

Простая аналоговая система, удобна на малых предприятиях, где нет необходимости в онлайн режиме просматривать данные. Данная система масштабируема в рамках одного предприятия. Не подходит для организаций с большим объемом данных (Рисунок 1.25).

Рисунок 1.25 – Аналоговая система видеонаблюдения

Гибридная система видеонаблюдения построена на аналоговой системе видеонаблюдения. За счет добавления оборудования для переработки аналогово сигнала в цифровой. Не подходит для предприятий со сложной иерархической структурой сети. Очень долгое время отклика конечных устройств (Рисунок 1.26).

Рисунок 1.26 – Гибридная система видеонаблюдения

IP система видеонаблюдения проста в установке. Легко масштабируема в любую сеть предприятия. Возможность просмотра данных онлайн, а так же

архивных данных. Просмотр данных с видео стены при получение определенных прав доступа (Рисунок 1.27).

Рисунок 1.27 – IP система видеонаблюдения

1.6.6 Интегрированные системы безопасности

Задачи

Системы IP–видеонаблюдения находят все более широкое применение в системах обеспечения безопасности и защиты. Использование IP–сетей открывает поистине безграничные возможности доступа к видео в записи и в реальном времени. В современных условиях необходимы дополнительные меры, обеспечивающие:

– управление большим числом видеосистем, включающих видеокамеры, устройства хранения, локальные и удаленные объекты наблюдения, с учетом ограничений пропускной способности сети;

– предоставление защищенного доступа пользователям из разных точек для более тесного взаимодействия;

– поддержку устройств и приложений (управляющих, видео аналитических и т.д.) разных производителей;

– интеграцию видео с другими сетевыми приложениями.

Решение

Система видеонаблюдения Cisco (VSM) позволяет администраторам сети и специалистам по системной интеграции создавать сеть видеонаблюдения в полном соответствии с имеющимися требованиями. Комплект программного обеспечения позволяет строить масштабируемые, настраиваемые и простые в управлении видеосистемы с возможностью доступа к видео в режиме реального времени или в записи в любом месте, в любое время, с использованием интерфейса Web–браузера, на компьютерах, КПК и смартфонах.

Работа под управлением операционной системы Linux, аппаратное обеспечение и сетевые IP–протоколы, имеющиеся в стандартной конфигурации, обеспечивают совместимость с большим числом устройств и приложений сторонних производителей. Авторизированные сетевые пользователи могут просматривать видеоданные с любого количества IP– или аналоговых камер с подключенным энкодером и управлять ими в режиме реального времени. При этом возможно использование различных отказоустойчивых опций записи и хранения данных с целью их восстановления в случае аварии. Набор функций системы видеонаблюдения может увеличиваться при внедрении новых технологий, когда у предприятия появятся соответствующие коммерческие возможности (Рисунок 1.28).

Кодирующий сервер (ES)

Кодирующий сервер (ES) системы видеонаблюдения Cisco – устройство типа «все в одном», осуществляющее кодирование, распределение, архивацию источников цифровых видеосигналов и управление ими.

Каждый сервер кодирует до 64 каналов и имеет до 9 ТБ памяти для хранения данных.

Возможности кодирующего сервера (ES):

– поддержка широкого диапазона аналоговых и IP–камер;
– одновременное кодирование в форматы M–JPEG и MPEG–4;
– циклическая запись видео и запись при наступлении события;
– возможность установки внешнего устройства хранения данных;
– обнаружение движения, тревожные входы, PTZ.

Рисунок 1.28 – Система видеонаблюдения Cisco VSM

Медиа–сервер видеонаблюдения (MS)

Медиа–сервер видеонаблюдения Cisco (Рисунок 1.29), (MS) – центральный компонент VSM, выполняющий распределение, архивацию данных от источников видеосигнала и управление их работой. Он обладает возможностями гибкой настройки и совместим с другими приложениями в IP–сети.

Возможности управления видеонаблюдением:

– Стандартизированная архитектура, гибкая настройка при работе с камерами, кодерами, устройствами просмотра и топологий сети.

– Видео с низкой задержкой и высоким качеством изображения, разрешение видеокамеры – 1 мегапиксель.

– Одновременная поддержка M–JPEG, MPEG–2 и MPEG–4.

– Масштабируемость количества площадок видеонаблюдения, камер, инструментов просмотра и устройств хранения.

Гибкая система архивации:

– Настраиваемая частота кадров, продолжительность и расположение архивных данных.

– Резервная архивация видеоданных в нескольких местах для снижения нагрузки на сеть.

– Возможность циклической записи и при наступлении определенного события, а также кадрирование видео и аудиоданных.

Расширенные средства системного управления:

– Улучшенные инструменты диагностики, обеспечивающие поддержку уведомлений и API в случае отказа прокси–серверов и архивов.

– Простая настройка, возможность синхронизации MS с APM оператора (OM) одним щелчком мыши.

– Поддержка настроек резервирования, включающих сценарии переключения при отказе и обеспечения бесперебойной работы.

– Минимизация нагрузки на платформы серверов видеонаблюдения посредством передачи только активных видеоканалов.

– Интеграция с системами управления электронным доступом других поставщиков (Lenel).

Рисунок 1.29 – Медиа–сервер видеонаблюдения

Система хранения данных видеонаблюдения Cisco

Система хранения данных видеонаблюдения Cisco (SS) использует экономичные настраиваемые устройства хранения видео– и аудиоданных с различным объемом памяти. Она объединяет внутреннее хранилище Медиа–

сервера с системами хранения DAS, SAN и NAS, обеспечивая хранение данных в разных местах и улучшая их доступность и защищенность. Видеоданные могут записываться циклично или по внешней команде, долгосрочно храниться в виде резервного архива на удаленном сервере.

Особенности Системы SS:

– Настройка систем хранения SAN, NAS и DAS.
– Объем внутренней памяти до 24 ТБ (на Медиа–сервере).
– SAN–массивы – до 42 ТБ в массиве, до 420 ТБ в стойке.
– Резервные архивы.
– Конфигурация RAID 0/1/5.
– Настраиваемая кластеризация для восстановления при отказе.
– Резервные источники питания и raid–контроллеры решения Cisco для видеонаблюдения.

Преимущества системы видеонаблюдения компании Cisco

Система видеонаблюдения VSM разработана на основе промышленных стандартов Cisco и позволяет организовать мощную, масштабируемую систему безопасности, отвечающую любым требованиям пользователей, включая совместимость с широким спектром продуктов других поставщиков (видеокамер, систем управления, контроля и анализа видеоданных, систем контроля доступа, серверов и устройств хранения данных). Комплект программного и аппаратного обеспечения, поставляемый в составе решения Cisco, периодически обновляется и дополняется новыми функциями. Технологии и знания Cisco в области разработки IP–сетей помогают организациям быстро окупать инвестиции и снижать совокупную стоимость владения видеосистемой. Имея огромный опыт работы с системами цифрового видео, включая видеонаблюдение, инженеры Cisco используют мощности IP–сетей для внедрения новых перспективных технологий, отвечающих требованиям безопасности. Система видеонаблюдения Cisco VSM может быть установлена на транспорте, в аэропортах, портах, в военной сфере, в образовательных учреждениях, в системе управления городским хозяйством, в магазинах розничной продажи и других областях (Рисунок 1.30).

Сервер обработки данных

Видеонаблюдение становится тесно вплетенным звеном IP сети. Сеть это платформа для подключения всех компонентов физических систем безопасности к другим корпоративным узлам и системам. Cisco Video Surveillance Manager (VSM) собирает данные со всех камер в одно место для записи и хранения.

Cisco VSM предоставляет комплексное решение для видеонаблюдения.

Менеджер видеонаблюдения Cisco включает в себя несколько компонентов, которые объединяются в общую сеть, чтобы создать гибкую, высоко масштабируемую систему для предприятия.

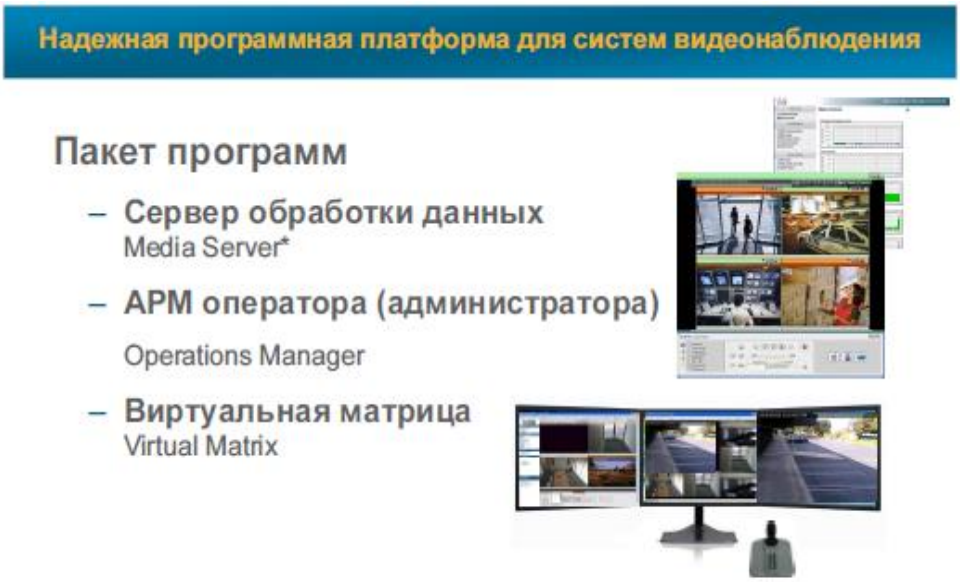


Рисунок 1.30 – Программное обеспечение Cisco VSM

Cisco Video Surveillance Operations Manager

Менеджер видеонаблюдения позволяет эффективно и результативно настраивать видео камеры всего предприятия. Так же VSM обеспечивает безопасный веб–портал для настройки, управления, отображения и управления видео (Рисунок 1.31).

Рисунок 1.31 – Менеджер видеонаблюдение Cisco

Cisco Operation Manager,Сервер АРМ операторов(администраторов) (Рисунок 1.32).

Функции которые выполняет Operations Manager:

1 Настройка оборудования.
2 Управление записью видеопотоков.
3 Управление пользователями и правами.
4 Управление виртуальными матрицами.
5 Управление о тревогах.
6 Вывод видеопотоков, настраиваемый пользовательский интерфейс.
7 Управление поворотными камерами.
8 Проигрыватель архива.

Рисунок 1.32 –Сервер обработки данных

Cisco Video Surveillance Media Server

Cisco Video Surveillance Media Server, выполняет следующие сетевые функции системы видеонаблюдения:

– Распределенная обработка всех видео, аудиоинформации о событиях.
– N + 1 резервирование.
– Сбор и маршрутизации видео со всех камер и передача информации по сети на сервер.
– Возможность безопасного хранения видео в архиве.
– Пометка событий и архивирование.
– Запись видео при обнаружения движения благодаря В–системе.
– Управление пропускной способностью записи камер.

Используя мощь и продвинутые возможности IP сети, программное обеспечение Cisco Video Surveillance Media Server позволяет через приложение, пользователям, просматривать архивную информацию в течение долгого времени. Программа предоставляет гибкую и масштабируемую систему для поддержки аналоговых систем видеонаблюдения:

– Развертывание которой варьируются от небольших систем до систем с тысячами камер.
– Оптимизация пропускной способности и вычислительных ресурсов с помощью Dynamic Proxy.

– Сотни одновременных пользователей с доступом живого и архивного видео.

– Стандартные видеокодеки, такие как Motion JPEG, MPEG–4 и H.264 одновременно в одном медиа–сервере.

– Сохранение с помощью событий, обрезки, запись на движения.

– Гибкие варианты развертывания, начиная от модулей в рамках Cisco.

Сервер обработки данных Media Server (Рисунок 1.33).

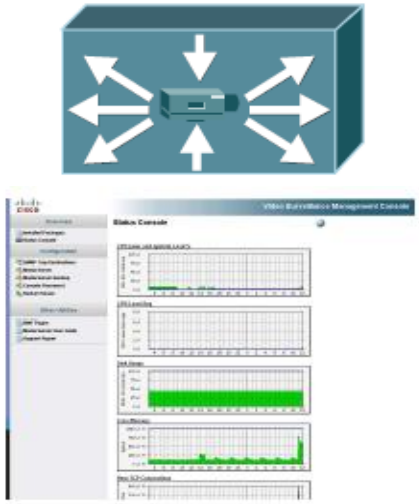


Рисунок 1.33 – Сервер обработки данных Media Server

Ключевые компоненты системы IP–видеонаблюдения:

1 Видео движок позволяет запись, удаление, передачу видео клиентам, со всех видеопотоков.

2 Высокая масштабируемость камер, клиентов, хранилищ.

3 Одновременная поддержка различных форматов кодирования: MPEG2, MPEG4, MJPEG, H.264.

4 Поддержка камер с мегапиксельным разрешением.

5 Гибкая настройка схем записи видеопотоков: темп записи, длительность, размещение, запись по событиям, запись по расписанию.

6 Средства мониторинга самого сервера и подключённых источников видеоданных.

Cisco VSM: Виртуальная матрица Virtual Matrix

Cisco в сфере физической безопасности обеспечивают широкие возможности и решения благодаря использованию технологии видеонаблюдения, IP камер, электронной системы контроля доступа и новаторских технологий. Решения Cisco в обеспечении физической безопасности, позволит заказчикам использовать IP сеть как открытую платформу для создания более широкого взаимодействия. Интегрированные системы, сохранят при этом уже существующие аналоговые системы. Благодаря этому клиенты начинают использовать IP сеть в качестве

платформы, для построения своих систем. Они могут получить значительную ценность за счет быстрого доступа к соответствующий информации и взаимодействовать между системами. Благодаря этому создастся более высокий уровень осведомленности и позволит принимать решения быстрее и более интеллектуально.

В качестве компонента в Cisco для решения проблем с видеонаблюдением используется диспетчер видеонаблюдения Cisco Virtual Matrix. Который позволяет авторизованным менеджерам и операторам просматривать и отображать видео с удаленных камер.

Видеонаблюдения Cisco Virtual Matrix (Рисунок 1.34), использует IP сеть, чтобы обеспечить агрегацию и передачу видео с камер и записывающих платформ. Программное обеспечение может выполнять функции классического аналогового переключателя видео матрицы, предлагая возможности, которые аналоговые переключатели не могут предоставить. Virtual Matrix предоставляет видео онлайн и уже записанное, обеспечивая доступ к сети видео для просмотра видео в формате 24x7. Операторы могут выбирать из доступных камер, которые будут отображаться на мониторах системы в пределах настраиваемых шаблонов отображения видео. Virtual Matrix легко интегрируется с другими системами для автоматического отображения видео.

1 Выводом заданных видеопотоков из IP сети.
2 Поддержка «живого» и архивного видео.
3 Управление выводом на видеостены.

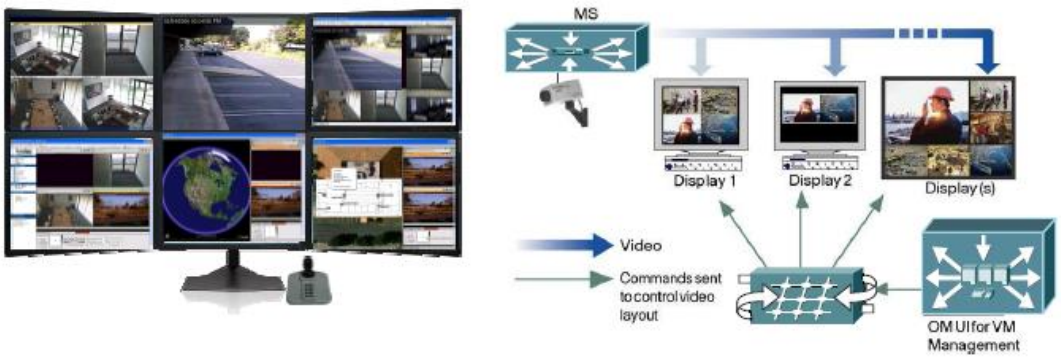


Рисунок 1.34 – Virtual Matrix

Ответная реакция на нарушения.

Система ответной реакции на нарушения Cisco использует IP сеть как платформу на которой разворачиваются крупномасштабная система неотложной помощи при происшествиях. В эту систему входит P25/VHF/UFH, PTT радиостанции, шлюз P25 ISSI, 1RU, 2RU серверные платформы, IP Dispatch Console, ПО IPICS Server, ПО для P25 ISSI шлюза, мобильный клиент, приложение для IP телефонов PTT. Система ответной реакции на нарушения Cisco представлена на рисунке 1.35.

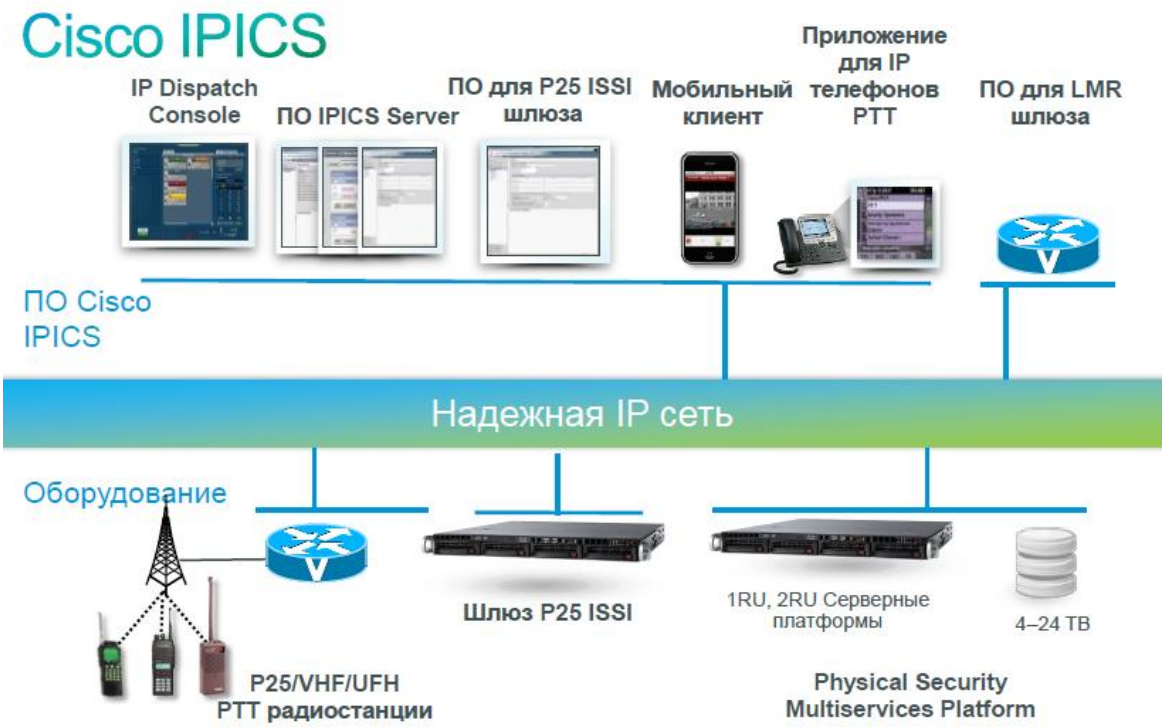


Рисунок 1.35 – Система ответной реакции на нарушения Cisco

Система (IPICS) решает и упрощает операции радио связи между диспетчерами и улучшает реакцию на инциденты, чрезвычайные ситуации. Cisco IPICS убирает коммуникационные барьеры между системами мобильной радиосвязи и устройств, таких как мобильные телефоны, стационарные телефоны, IP–телефоны. Она поддерживает связь между пользователями всех устройств, где бы они небыли расположены.

Когда время имеет решающее значение, Система (IPICS) предоставляет информацию в нужные руки в нужное время и в нужном формате. Система (IPICS) повышает ценность существующих и новых радиостанций, телефоний, и сетей IP связи.

Система Cisco IPICS.

На рисунке 1.36 показана система взаимосвязи IPICS.

Система Cisco IPICS состоит из нескольких аппаратных и программных компонентов.

Консоль диспетчерского управления Cisco IPICS Dispatch Console:

– Объединение в группы любых устройств.

– Отправка видео, картинок, звука и другой информации.

– Допускает использование любых радио сетей и позволяет облегчить миграцию на новые протоколы (P25, Tetra).

IPICS отправляет данные на консоль радио–диспетчера. Она предназначена для связи всех радио точек с критически важными данными. Система (IPICS) является важным звеном между диспетчерами и персоналом

работающих на отдаленных местах. Помогает координировать реакцию персонала на сложные ситуации.

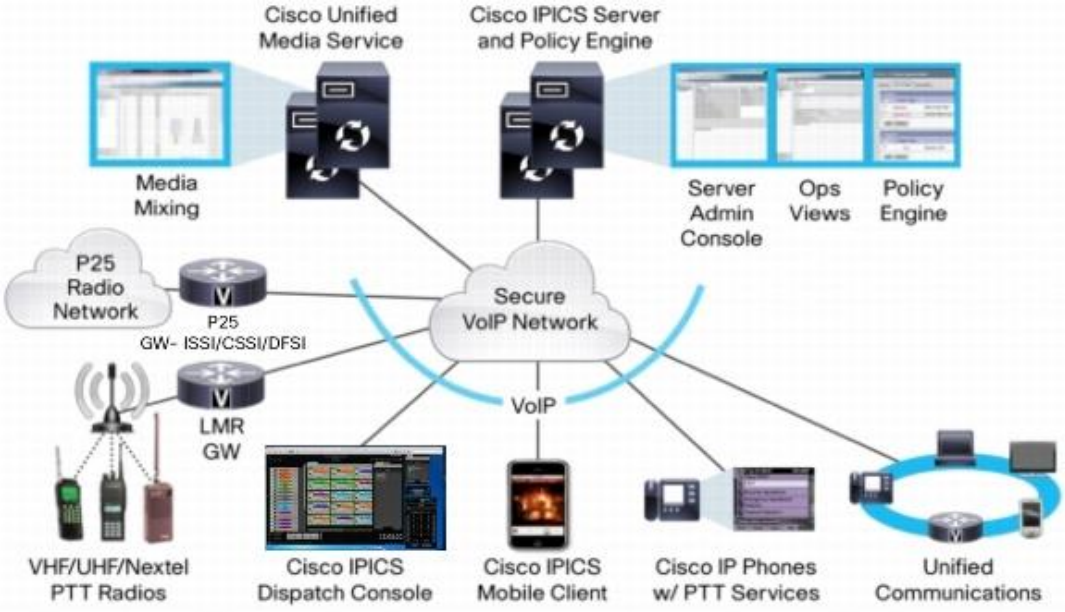


Рисунок 1.36 – система взаимосвязи IPICS Cisco

Консоль диспетчерского управления Cisco IPICS Dispatch Console работает на стандартной платформе ПК. Она расширяет существующие Push–To–Talk (PTT) радиоканалы, так что пользователи с различными коммуникационными устройствами могут участвовать в мероприятии. Cisco IPICS обеспечивает контроль ресурсов радиосвязи через легкий в использовании интерфейс (Рисунок.1.37).

Рисунок 1.37 – Консоль диспетчерского управления Cisco IPICS Dispatch Console

Диспетчеры могут отслеживать и координировать рабочий персонал на чрезвычайные ситуации через системы радио–канала.

Интуитивно понятный графический интерфейс обеспечивает доступ ко всем функциям отправки, в том числе:

– PTT и мониторинг до 50 радиоканалов и разговорных групп.

– Встроенный клиент телефонии до 10 линий для входящих и исходящих вызовов.

– Push–To–Talk (PTT) радиоканалы.

– Экранный показатель активности канала.

– Телефонную трубку, гарнитуру или настольный микрофон.

– Индивидуальный канал отключения.

– Все разговоры.

– Мгновенная запись.

– Последний звонок.

– Сигнала о приеме.

– Аварийное оповещение.

– Выбор частоты.

– Шифрование.

Консоль диспетчерского управления Cisco IPICS Dispatch Console интегрируется практически с любым аналоговым или цифровым радиосистемами. Он вводит многофункциональную интерактивную медиа–поддержку. При возникновении инцидента, он дает диспетчерам власть консолидировать информацию и мгновенно делиться этой информацией среди рабочего персонала.

Реагирование на инцидент поддерживает совместное использование мультимедийных данных, в том числе:

– Онлайн видео отправленное с камер наблюдения, контроля доступа шлюзов и мобильных клиентов.

– Архивные видео.

– Фотографии.

– Мониторинг аварийных сигналов.

– Журнал и живые статусы.

– Веб–ссылки на ресурсы, такие как FEMA.

– IPv4 IP Соответствие (IANA).

Новой стандарт в IPICS 4.6

Cisco IPICS 4.6 включает в себя следующие основные новые функции:

– *Совместимость радиосетей* – эта версия поддерживает Интер–RF Subsystem Interface (ISSI), Console Subsystem Interface (CSSI) и ТИА P25 Цифровой стационарной станции Интерфейс (DFSI.

– *DFSI шлюз* – этот релиз включает в себя новую P25 DFSI шлюз.

– *Поддержка менеджера видеонаблюдения Cisco 7* видео менеджер может быть интегрирован с IPICS отправка данных на консоль.

– *TETRA радио* – эта версия поддерживает конфигурацию и использование TETRA радиостанций.

– *SNMP* новая вкладка SNMP в Cisco IPICS Administration Console – позволяет настроить параметры SNMP V2 для Cisco IPICS.

– *Поддержка языка* – поддержка интернационализации IPICS.

– *IP–телефон Cisco дает высокую доступность* – IPICS поддерживает IP телефон клиента.

– *Обновлен Cisco Unified Communications Manager поддержка* – эта версия поддерживает Cisco Unified 9.x. менеджер по коммуникациям.

Консоль диспетчерского управления Cisco IPICS Dispatch Console особенности – новые или обновленные функции в IPICS диспетчерской консоли включают в себя:

– *Отрываемый предметы* – Вы можете настроить внешний вид консоли, перемещая различные предметы из главного окна в любое место на экране компьютера.

– *Адресная книга* – Вы можете получить доступ и управлять несколькими списками контактов и быстро позвонить или отправить электронную почту контакту.

– *Не беспокоить* – входящий вызов будет обрабатываться таким образом, что функция DND настроенного в Cisco Unified Communications Manager,.

Сенсорная панель IP Cisco IPICS

Сенсорная панель IP Cisco IPICS является новой возможностью IPICS, предоставленная партнером Cisco SolutionsPlus. Это новая консоль поддерживающая расширенные возможности в управлении инцидентами и телефонными функциями, такие как приоритет вызова очереди, несколько логические линии. Эти возможности интегрированы с Cisco Unified Communications, что позволяет диспетчерам выставлять приоритеты своей работы и добиться более высокой производительности.

Сенсорная панель IP Cisco IPICS (Рисунок 1.38) является полным диспетчерским приложением со встроенным аудио и видео функциями.

Рисунок 1.38 – Сенсорная панель IP Cisco IPICS

Мобильный клиент Cisco IPICS

Происшествия может произойти где угодно и в любое время. Приложение мобильный клиент Cisco IPICS передает данные в реальном времени с мобильного телефона на консоль. Пользователи могут использовать IPICS Mobile Client, что бы передавать свои собственные видео и фотографии с происшествий, мгновенно делая информацию доступной для всех участников сети (Рисунок 1.39).

Рисунок 1.39 – Cisco IPICS Мобильный Клиент

Высокая доступность

Система IPICS имеет возможность добавления вспомогательного резервного сервера для UMS и IPICS, чтобы обеспечить высокую доступность и безотказность. Если не удается подключиться к первичному серверу, вторичный сервер автоматически берет на себя обслуживание без прерывания связи. Серверы могут быть географически разделены или находится в одном месте. Административные функции и журналы данных синхронизированы, чтобы избежать потери информации.

Улучшенная IPICS API

API веб–сервис интегрируется с IPICS, для командования и управления информацией, физической безопасности (PSIM) и автоматизированных приложений диспетчеризации.

Таблица 1.4 показывает возможности Cisco IPICS.

Таблица 1.4 – IPICS Возможности системы

Возможности системы	Спецификация
IPICS пользователи в базе данных	До 50000
Активные пользователи	До 1000
Активные диспетчерские консоли	До 250
VTGs	До 150 активно
Радио каналы	До 1500 активных каналов
Dial–In/Dial–Out Пользователи	До 200 пользователей активные набора
Мобильные клиенты	До 1000 активен (включен в Active Users выше)

Лицензирование информации

Сервер Cisco IPICS проверяет число лицензий программного обеспечения. Лицензия требуется для каждого клиента IPICS. Cisco IPICS может быть установлена на многих ПК. В таблице 1.5 представлены варианты лицензирования.

Таблица 1.5 – IPICS Лицензии

Пакет	IPICS4.X–BDL1–K9	IPICS4.X–BDL2–K9	IPICS4.X–BDL3–K9
IPICS сервер лицензий	1	1	1
Виртуальные Обсуждение Группы	1	10	50
Политика двигателя	1	0	1
Порты радиоканалу	2	8	10
Серебряные Консоли	1	10	10
Платиновые Консоли	0	4	4
IP–телефоны	1	10	10
Наберите портов	1	10	10

Коммуникационные возможности изменились с распространением технологий IP следующего поколения. Cisco IP Interoperability предназначен для интеграции традиционных диспетчерских систем с новыми технологиями, улучшает осведомленность в сложной ситуации. Когда время имеет решающее значение, Cisco IPICS помогает доносить информацию до нужных людей в нужное время, в нужном формате. Cisco IPICS Мобильный Клиент является новым компонентом решения Cisco IPICS.

Особенности и преимущества

До недавнего времени рации были самыми доступными средствами коммуникации. Тем не менее, они в основном сводятся к аудио информации, конечно, эта технология ограничена. Рации как правило имеются только у дежурных групп. А мобильный смартфон с возможностью подключения к интернету может быть доступен из любой точки в мире.

Эффективное использование, смартфона может повлиять в качестве хорошего дополнения к обычным радио станциям где необходимо передавать аудио и видео информацию. Cisco вводит мобильный клиент IPICS для решения этой возможностью.

Мобильный Клиент IPICS это приложение, которое позволяет реагировать и взаимодействовать с другими участниками происшествия. С помощью этого приложения можно динамически добавлять свои собственные видеоклипы, фотографии и обновления статуса. IPICS мобильный клиент используется в сочетании с IPICS диспетчерский консоль. Обеспечивает по требованию решение для физической безопасности и чрезвычайных служб быстрого реагирования. Это дает возможность начать рассмотрение информацию об инцидентах и решать находясь в пути к месту происшествия. Они больше не привязаны к настольным компьютерам, ноутбукам или радио UHF / VHF (Рисунок 1.40.)

Рисунок 1.40 – Cisco IPICS Мобильный клиент для Apple Iphone (три вида)

Использование в сочетании диспетчерской консоли IPICS и мобильного клиента IPICS позволяет мультимедийное сотрудничество между диспетчерами. В том числе в режиме реального времени обмена информацией, которая включает следующие пункты:

– Живое видео отправлено с камер наблюдения, шлюзы контроля доступа и мобильных клиентов.

– Архивные видео.

– Фотографии.

– Мониторинг аварийных сигналов.

– Журнал и живые статусы.

– Веб–сайт ссылки на ресурсы, такие как FEMA и опасных материальных баз данных, стандартных оперативных процедур и карт.

IPICS Мобильный Клиент берет понимание ситуации на новый уровень. Преимущества включают:

– *Мобильность:* IPICS мобильный клиент, на основе смартфонов, дает связь, где есть беспроводная сеть, например, Wi–Fi или 3G сотовой связи.

– *Радио взаимодействие:* IPICS мобильный клиент позволяет PTT взаимодействия с радиоканалами разговорных групп.

– *Rich Media:* В Cisco IPICS мобильный клиент выходит за рамки аудио поддержки устройств.

Основные возможности системы можно просмотреть на таблице 1.6

Таблица 1.6 – Возможность системы

Параметры	Значения
Платформы	Apple iPhone 3G / 3GS / 4 с прошивкой до 4,1; Ipad, Itouch
Связь	Wi–Fi или 3G
Связь со всеми	До 10 (рекомендуется для оптимальной производительности)
Живое видео	До 10 минут
Фото	До 2 МБ
Мобильный клиент	1000 мобильных клиентов в IPICS системы

Cisco® Physical Security Operations Manager

Cisco® Physical Security Operations Manager – это пульт управления оператора, он объединяет управление и работу менеджера по видеонаблюдению Cisco, шлюз физического доступа Cisco, систему функциональной совместимости и сотрудничества IP Cisco (IPICS).

Cisco® Physical Security Operations Manager собирает воедино все сигналы с датчиков, тем самым консолидирует всю информацию в единое расположение. На дисплеях простых в использовании программных продуктов обеспечивается эффективная визуализация данных и предоставляющий прямой доступ ко всем устройствам расположенных на карте событий.

Cisco® Physical Security Operations Manager приводит в действие сложных бизнес–логический механизм, позволяющий пользователям настраивать схемы по их нуждам, пересекающие все устройства и все датчики. И тем самым снизить риск потери информации (Рисунок 1.41).

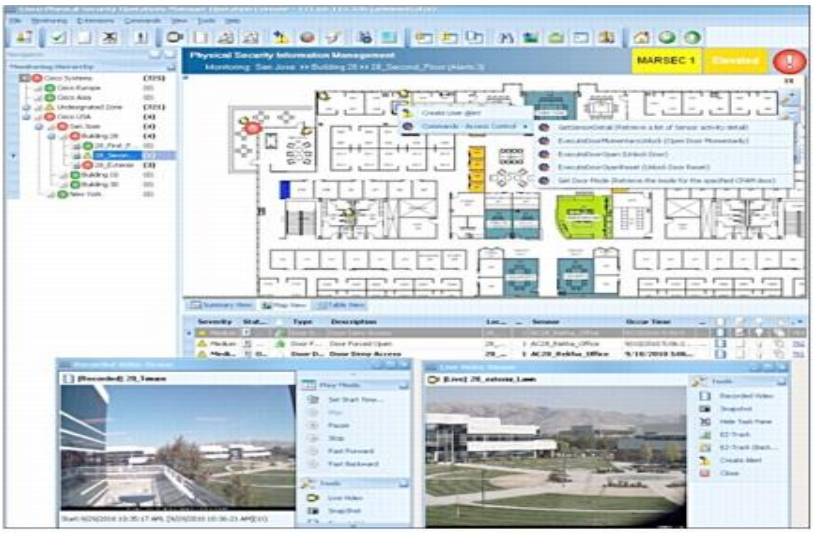


Рисунок 1.41 – Cisco Physical Security Operations Manager

Важные особенности

Центральная консоль с помощью которой можно управлять всеми сетевыми устройствами и иметь доступ к тысячами камер.

Менеджер операций физической безопасности Cisco обеспечивает масштабируемость, которая требуется для управления тысячами IP видео камер, через менеджер видеонаблюдения.

Интерактивные геопространственные карты. Менеджер операций физической безопасности Cisco обеспечивает полное представление об устройствах и датчиках в простом и интуитивном представлении. Операторы на карте здания предприятия могут просматривать зоны безопасности. Тем самым открывая интересующую их охраняемую зону и просматривая все датчики в ней.

Управления датчиками безопасности, устройствами и ресурсами. Интерактивные карты позволяют операторам просматривать данные с IP камер

или шлюза физического доступа и брать на себя управление через интерфейс Cisco Physical Security Operations Manager. Операторы в состоянии выполнить широкий диапазон действий в их сети. Они могут просматривать живое видео и уже записанное в архив, беря под свой контроль камеры PTZ, выполняемыми дверными шлюзами контроля доступа.

Video matrix и видео тур. Видеопотоки могут быть представлены оператору в отдельных окнах или в матричном представлении (Рисунок 1.42). Видеоокна могут также быть сконфигурированы, с любых камер подключенных с сети.

Центральная сигнализация. Централизованная консоль позволяет сгенерировать аварийные сигналам и автоматически показывать их на карте. На основе пользовательских настроек сигнальные детали могут быть автоматически выведены на экран или выведены на экран оператором горячими клавишами мыши.

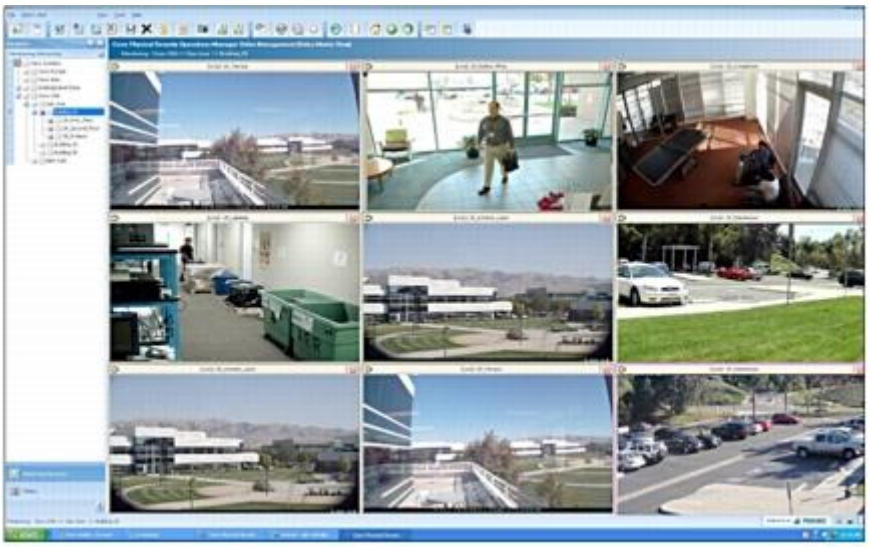


Рисунок 1.42 – Видеопотоки с камер в матричном пространстве 3x3

Оценка инцидентов и бизнес–логики

Менеджер операций физической безопасности Cisco разумно соединяет и коррелирует события безопасности и аварийные сигналы, минимизируя ложные аварийные сигналы, позволяя службе безопасности работать в режиме реального времени после поставки на охрану предприятия. Операторы мгновенно видят все детали чрезвычайных аварийных ситуаций, тем самым не требуется полная остановка работы предприятия для решения аварийной ситуации.

Информация, доступная операторам, включает в себя:

– Детали сигнализации. Предоставляет определенную информацию об аварийных сигналах. Система, которая включает аварийный сигнал и показывает место сигнала на карте.

– Живое и архивное видео. Видео, записанное от начала рабочего дня и до случившейся аварийной ситуации.

– Ответная реакция диспетчера. Система обеспечивает инструкциями оператора о случившейся чрезвычайной ситуации. Чтобы передать сигнал на пульт дежурной охраны.

– Примечания оператора. Страница примечаний позволяет операторам записывать дополнительные сведенья, связанные с аварийным сигналом.

– Управление системой обеспечения безопасности. Эта система позволяет операторам принять ответные меры, просмотрев информацию с камер, они могут блокировать двери, чтобы временно блокировать/разблокировать дверь.

– Создание отчетов. Службы безопасности могут создать консолидированные сообщения о происшествии (инцидентные досье) и экспортируемое видео. Эти отчеты могут использоваться для создания отчетов управления или судебных целей, и они включают все сигнальные детали, фотографии, попытки доступа, миникарты и видеофайлы.

Бизнес–логика используется, чтобы передать или фильтровать аварийные сигналы на основе предопределенной информации. Когда аварийные сигналы будут переданы, менеджер операций физической безопасности будет передавать информацию на дисплей оператора с определенными инструкциями, которые должны быть применены, в определенной аварийной ситуации. Бизнес–логика созданная на основе шаблонов позволяет персоналу службы безопасности выполнять запланированный за ранее план по урегулированию чрезвычайных ситуаций (Рисунок 1.43).

Рисунок 1.43 – Оценка инцидентов и бизнес–логики Builder

Усовершенствованное создание отчетов

Усовершенствованный многофункциональный модуль сообщений позволяет операторам безопасности, супервизорам и менеджерам отслеживать аварийные сигналы по времени, датчику, расположению и типу, чтобы упростить работу службе безопасности.

– Создание отчетов о происшествии. Простой в использовании, управляемый мастером механизм создания отчетов быстро генерирует отчеты на основе аварийных сигналов, сгенерированных в системе.

– Предопределенные отчеты. Менеджер операций физической безопасности Cisco обеспечивает множество отчетов для общих запросов, позволяет быстро просматривать информацию и делать важные решения.

Конфигурация из нескольких серверов которые можно подключить к одной системе (Рисунок 1.44).

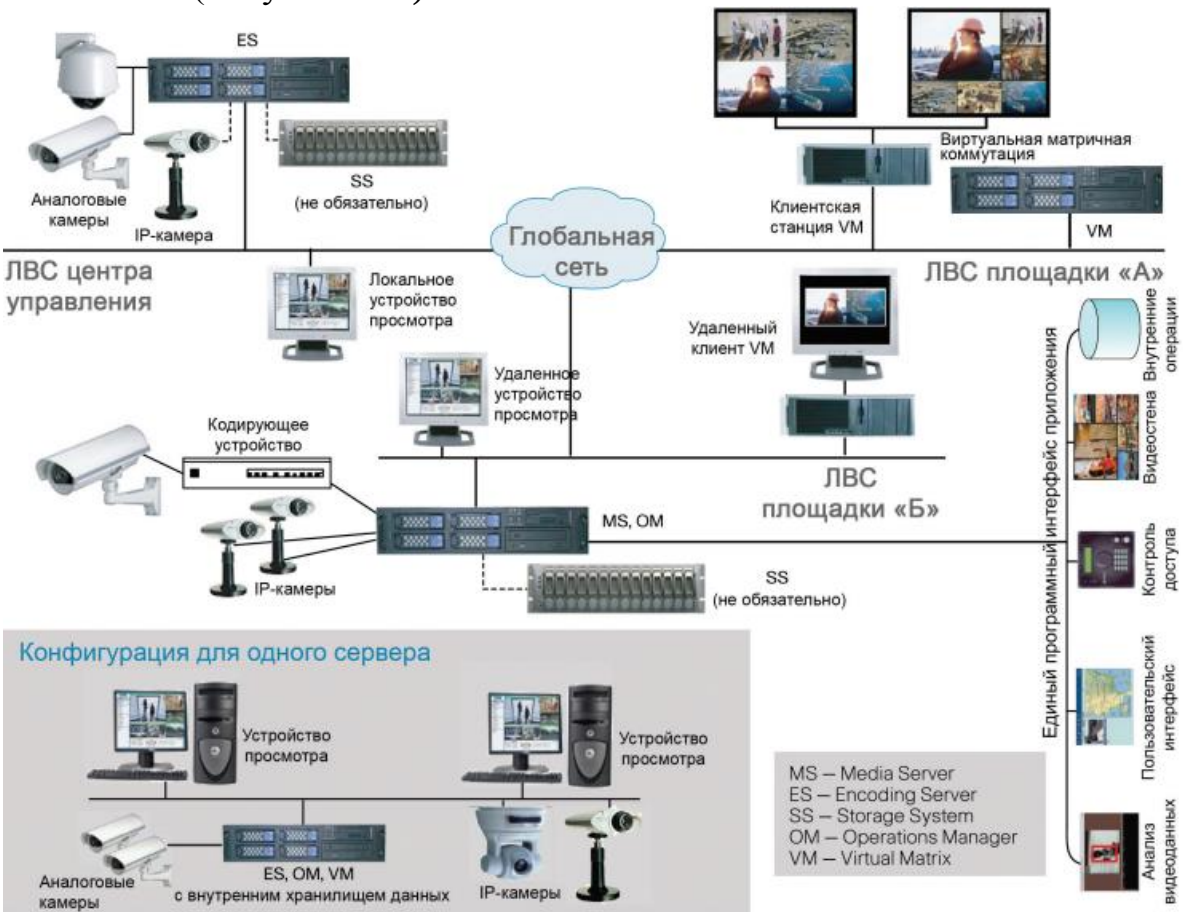


Рисунок 1.44 – Конфигурация для нескольких серверов

2. Конструкторская часть

Инженерно–техническая защита (ИТЗ) – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Структура технической части в доле обеспечения требуемого уровня безопасности на объекте неоднозначна и разбивается на две подсистемы: комплекс защитных сооружений и инженерных конструкций (средства инженерной защиты) и собственно, технические средства обеспечения (средства технической защиты).

Средства инженерной защиты – разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.

Комплекс защитных сооружений и инженерных конструкций дополняет укрепленный периметр до полного в части выполняемых проемов, в т.ч. входов/выходов для обеспечения штатного и аварийного доступа, выполнения световых фонарей, защиты жизни работникам охраны, организации препятствий на путях силового прорыва транспорта, зон присутствия и разделения потоков посетителей и транспорта.

На долю настоящего комплекса в системе обеспечения безопасности объекта отводятся следующие основные функции:

– увеличения времени несанкционированного доступа на объект, в т.ч. силового (в идеале – с момента обнаружения неправомерных действий до потребной организованной реакции должно пройти времени гарантированно меньше, чем нужно для организации пресечения этих действий при максимально возможной угрозе);

– пресечения и подавления неправомерных действий (вкупе со специальными средствами);

– сохранения жизни работникам патрульно–постовой службы и команде реагирования.

Единственным и основным принципом в организации инженерной защиты объектов является достаточность и адекватность любой прогнозируемой угрозе.

Технические средства обеспечения – достаточно развитая номенклатура изделий, позволяющая резко снизить нагрузку на патрульно–постовую службу в части обнаружения неправомерных действий и в отдельных случаях подавления (газовое заполнение объемов, световое и звуковое психологическое воздействие, поражение электрическими зарядами).

В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача технических средств:

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещения.

Сюда относятся механические, электромеханические, электронные, электронно–оптические, радио– и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий (Рисунок. 2.1).

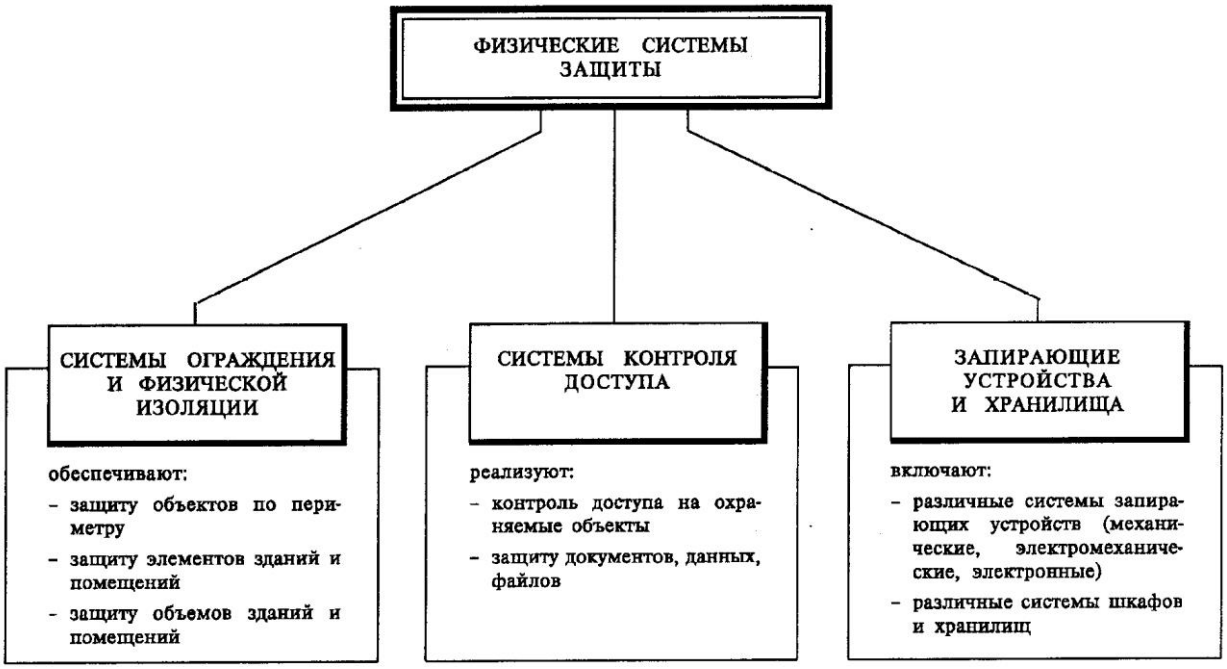


Рисунок 2.1 – Классификация физических средств защиты

2.1 Технические средства защиты

На сегодняшний день технические средства защиты достаточно разнообразны и в целом очень эффективны. Однако практически всем им присущ один существенный недостаток: они детектируют сигнал вторжения лишь после проникновения злоумышленника на территорию объекта. Простым примером тому служат системы охранного видеонаблюдения. Эти системы, в большинстве своем, при помощи видеорегистраторов способны лишь подтвердить факт вторжения после того, как он уже произошел. Зачастую злоумышленник рассчитывает на эту временную задержку, которая проходит с момента проникновения на объект до момента срабатывания сигнализации.

Коренным фактором, определяющим эффективность любой охранной системы, является минимизация этого интервала времени, и в этом смысле привлекательность периметральных систем охраны (ПСО) неоспорима. Периметральная граница объекта является наилучшим местом для раннего детектирования вторжения.

Нарушитель, взаимодействуя, в первую очередь, с физическим периметром, создает возмущения, которые и можно зарегистрировать специальными извещателями. Будь то ограждение в виде металлической решетки – ее надо перерезать или перелезть через нее, будь то стена или барьер – их придется преодолевать сверху, если это стена или крыша здания – их нужно разрушить, ну а если это открытая территория – ее нужно пересечь. Тем самым, физический контакт нарушителя с периметром, дает возможность электронными средствами обнаружить вторжение. Причем обнаружить именно на первом рубеже охраны, т.е. на периметре.

Считается, что периметральные системы охраны являются наиболее эффективными средствами защиты от несанкционированного проникновения, поскольку выдают сигнал тревоги задолго до того, как злоумышленник может проникнуть в особо важные зоны охраняемого объекта.

Прежде всего, любая такая система должна отвечать ряду критериев:

– возможность раннего обнаружения нарушителя, еще до того, как он проникнет на объект;

– отсутствие "мертвых" зон и по возможности точное следование контурам периметра;

– скрытая установка;

– невосприимчивость к изменениям климатических условий (таким, как температура, давление, влажность и т.д.);

– невосприимчивость к электромагнитным индустриальным помехам вблизи охраняемого объекта.

2.1.1 Система охранно–пожарной сигнализации

Одной из составляющих сложившегося понятия «Безопасность» являются системы охранно–пожарной сигнализации (ОПС). Вопросы совершенствования этих систем будут актуальны еще долгое время, о чем свидетельствует большое количество статей по данной тематике, постоянно появляющихся в периодической литературе.

Приемно–контрольные приборы (ПКП) – первооснова построения ОПС – делятся на три группы: малой (1–5 шлейфов), средней (от 6 до 50 шлейфов) и большой (более 50 шлейфов) информационной емкости. Каждая группа ПКП по своему назначению может быть разделена на три подгруппы: пожарные (ПКПП), охранно–пожарные (ПКПОП) и охранные (ПКПО). Каждая подгруппа имеет своего потенциального потребителя.

Требования к системе охранно–пожарной сигнализации объекта информатизации

В соответствии с нормами пожарной безопасности «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией» устанавливаются основные требования пожарной безопасности, регламентирующие защиту зданий, сооружений, помещений и оборудования на всех этапах их создания и эксплуатации автоматическими установками пожаротушения (АУПТ) и автоматическими установками пожарной сигнализации (АУПС).

В зданиях и сооружениях следует защищать соответствующими автоматическими установками все помещения независимо от площади, кроме помещений:

– с мокрыми процессами (душевые, санузлы, охлаждаемые камеры, помещения мойки и т.п.);

– венткамер (приточных, а также вытяжных, не обслуживающих производственные помещения категории А или Б), насосных водоснабжения, бойлерных и др. помещений для инженерного оборудования здания, в которых отсутствуют горючие материалы;

– категории В4 и Д по пожарной опасности;

– лестничных клеток.

Здания, сооружения и помещения, подлежащие оборудованию установками охранной и пожарной сигнализации, рекомендуется защищать охранно–пожарной сигнализацией.

Критерии выбора, выбор и физическая реализация системы

Выбор оборудования для противопожарных систем любого объекта всегда в той или иной степени проблема – нормативная, техническая, финансовая либо конъюнктурная. Но начинать, пожалуй, надо с технических вопросов.

При выборе оборудования наиболее актуальными требованиями с технической точки зрения являются надежность и совместимость отдельных приборов, функциональная достаточность системы в целом (без «белых пятен» и излишнего дублирования). Поэтому имеет смысл рассматривать приборы, по возможности, одного изготовителя т.к. это гораздо облегчит интеграцию подсистем и уменьшит финансовые затраты.

Приступая к работе, приоритетность разработок и их очередность решаются практически одновременно с разработкой общей концепции. Кроме таких общих факторов, как востребованность аппаратуры и насыщенность рынка, необходимо учитывать и частные, например, субъективные возможности фирмы.

Одним из ведущих решений в области разработки и производства приборов охранной, пожарной и охранно–пожарной сигнализации является Cisco: Датчик дыма Cisco sc460, Датчик движения, вибрации, температуры Cisco sc470, Датчик влажности Cisco sc510.

Планирование IP–адресаций

Для каждого пожарно–охранного датчика должно быть присвоено свое идентификационное имя, по которому его можно будет определить. Распределение IP адресации представлено в таблице 2.1.

Таблица 2.1 – Планирование IP – адресации для пожарно–охранной сигнализации

Датчики	IP – адрес/Маска	Шлюз
Дымовой пожарный извещатель sc460	192.168.10.2 – 41/24	192.168.5.1
Приемно–контрольный прибор sc470	192.168.10.42 – 59/24	192.168.5.1
Датчик влажности sc510	192.168.10.60 – 64/24	192.168.5.1
Всего:	60	

Схема построения датчиков пожарно–охранной сигнализации 1 и 2 этажа представлена в Приложении Б.

2.1.2 Телевизионная система видеоконтроля

Системы телевизионного наблюдения предназначены для обеспечения безопасности на объекте. Они позволяют наблюдателю следить за одним или несколькими объектами, находящимися порой на значительном расстоянии как друг от друга, так и от места наблюдения. В настоящее время системы телевизионного наблюдения не являются экзотикой, они находят все более широкое применение во многих сферах человеческой жизни. Наиболее простая система телевизионного наблюдения – это камера, подключенная к телевизору или монитору, такая система позволяет наблюдать за ребенком или автомобилем возле дома.

Электронные системы наблюдения позволяют выполнять и другие не менее важные и более сложные задачи. Например, наблюдение за несколькими больными одновременно, движением транспортных потоков на оживленных магистралях или в портах. Существует целый ряд применений систем видеонаблюдения в научных исследованиях и в промышленности, например, для контроля над технологическими процессами и управления ими. При этом наблюдение может производиться в условиях низкой освещенности или в средах, где присутствие человека не допускается. Успешно эти системы используются в магазинах, в казино, в банках, на автостоянках. Малокадровые системы для дома и офиса способствуют повышению безопасности и создают дополнительные удобства.

Однако основной задачей, с которой должна справляться система телевизионного наблюдения, и именно для этих задач они и создавались – это обеспечения физической безопасности объекта, как самостоятельно, так и при совместной работе с другими системами безопасности.

При современных темпах криминализации общества и роста преступности, сложившейся общественно политической обстановке в стране, постоянной угрозы террористических актов просто необходима охрана

периметра и территории, контроль доступа на объект его сотрудников, посетителей и транспорта, ведение визуального наблюдения за состоянием различных частей объекта.

Требования к телевизионной системе видеоконтроля

Применение телевизионного контроля позволяет в случае получения сигнала о нарушении определить характер нарушения, место нарушения, направление движения нарушителя и принять необходимые меры.

Телевизионными камерами ТСВ целесообразно защищать:

– периметр здания объекта и подъездные к нему пути;

– центральный вход на объект (как снаружи, так и с внутренней стороны);

– боксы, ворота для въезда машин;

– операционный, торговый, выставочный и кассовый залы;

– помещения, коридоры по которым производится транспортировка денег и материальных ценностей;

– другие помещения по усмотрению руководства и службы безопасности объекта.

Для наружного наблюдения рекомендуется использовать телекамеры, имеющие высокую чувствительность (не менее 0,5 люкса для хорошо освещенных участков местности или не менее 0,05 люкса для плохо освещенных).

При размещении камеры вне помещения ее рекомендуется устанавливать в водозащитном термокожухе с солнцезащитным экраном, защищающим от атмосферных осадков и низкой температуры.

При необходимости смены поля зрения не только путем изменения фокусного расстояния, объектива, но и посредством поворота самой камеры в горизонтальной и вертикальной плоскости следует применять поворотные устройства с телеуправлением.

Внутри здания объекта рекомендуется использовать недорогие миниатюрные камеры со встроенным объективом и укреплять их стационарно так, чтобы в охраняемом помещении не возникало мертвых зон.

Для отображения поступающей информации с камер ТСВ следует применять только специальные мониторы, способные работать круглосуточно в течение длительного времени и часто с неподвижным изображением и имеющие разрешающую способность не менее 600–700 ТВЛ (разрешение в телевизионных линиях).

При использовании ТСВ в качестве охранного рекомендуется использовать детекторы движения, которые превращают телевизионную систему наблюдения в дополнительный охранный извещатель, передающий сигнал тревоги в систему охранной сигнализации при появлении в поле зрения активного или движущего объекта.

Физическая реализация телевизионной системы видеоконтроля

Можно выделить основные преимущества систем видеонаблюдения перед другими средствами безопасности. Это автоматическое обнаружение и

видео контролирование событий, мгновенное обнаружение несанкционированного проникновения на охраняемую территорию, исключение ложных срабатываний за счет интеллектуальной обработки поступающих информационных потоков, наглядное отображение всей обрабатываемой информации, возможность тесной интеграции с другими подсистемами безопасности.

Основными критериями систем видеонаблюдения при их разработке являются надежность, информативность, достоверность и своевременность.

Первый критерий достигается при использовании только самых лучших компонентов от ведущих мировых производителей, использованием проверенных на практике и глубоко продуманных конструктивных решений. Все это позволяет достигнуть наибольшего времени работы системы между отказами и минимального периода восстановления.

Соблюдение второго критерия позволяет обеспечить одновременную и непрерывную работу видеодетекции движения, видеозаписи, отображения на экран, воспроизведения и резервного архивирования по каждой из подключенных камер.

Достоверность – основной критерий для оператора системы и работников службы безопасности объекта, на котором установлена система видеонаблюдения. Достигается путем минимизации ложных срабатываний за счет интеллектуальных алгоритмов обработки потоков видеоинформации, увеличения изображения при условиях недостаточной видимости.

Своевременность обеспечивает прямой доступ авторизованных лиц к видео архивам, показ предыстории событий т.е. видеозаписи которая была получена за несколько секунд до срабатывания тревоги, возможность принятия решения системой самостоятельно без участия оператора.

В настоящее время используется два принципа построения систем видеонаблюдения: аналоговые и цифровые. Одним из ведущих предприятий в области разработки и производства приборов видеоконтроля является Уличная сетевая беспроводная видеокамера Cisco 2500W, Купольная IP камера 5010,5011.

Планирование IP–адресаций

Для каждой камеры должно быть присвоено свое идентификационное имя, по которому его можно будет определить. Распределение IP адресации для камер представлено в таблице 2.2.

Таблица 2.2 – Планирование IP – адресации для систем контроля видео наблюдения

Датчики	IP – адрес/Маска	Шлюз
Беспроводная видеокамера Cisco 2500W	192.168.11.2 – 7/24	192.168.6.1
Купольная IP камера 5010,5011	192.168.11.8 – 38/24	192.168.6.1
Всего:	35	

Схема построения IP камер 1 и 2 этажа представлена в Приложении В.

2.1.3 Система контроля и управления доступом

Системой контроля и управления доступом (СКУД) называется совокупность программно–технических средств и организационно–методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта.

Действительно, СКУД это не только аппаратура и программное обеспечение, это продуманная система управления движением персонала.

СКУД предназначена для автоматизации процесса управления доступом на режимные объекты предприятия (объекты охраны). В качестве контролируемых объектов могут выступать здания, этажи, отдельные помещения или огороженные участки территории. Средства СКУД позволяют управлять одновременно целым комплексом контрольно–пропускных пунктов различного типа: дверями, воротами, проходными.

Будем считать, что СКУД является третьим рубежом защиты после системы охранно–пожарной сигнализации и системы видеонаблюдения, но ни в коем случае не заменяет бдительных сотрудников службы безопасности и не исключает необходимость закрывать двери. Хотя бы потому, что основная задача СКУД – регламентировать передвижение сотрудников и посетителей в рабочее время и предотвращать попадание нежданных гостей в охраняемые помещения.

Несмотря на уникальность каждой конкретной системы, есть и будут существовать "три кита", без которых ограничение доступа попросту невозможно:

- управляющие контроллеры;
- устройства идентификации личности;
- оборудование ограничения доступа.

СКУД предоставляет следующие возможности:

- гибкое определение состава и схемы развертывания СКУД на объектах охраны с использованием стандартных средств, предоставляемых локальными сетями;
- создание иерархической структуры объектов охраны (каждый такой объект может содержать индивидуальный набор контроллеров, администраторов, операторов, пользователей и планов доступа);
- многопользовательский режим доступа к средствам СКУД, разграничение полномочий операторов и регистрация всех их действий; автоматизированное ведение учета прав доступа пользователей (регистрация, удаление, изменение полномочий), гибкая система задания графика движения пользователя через контроллер, выдача трех видов пропусков (постоянных, временных и разовых);

– ведение журналов и протоколов событий, происходящих в системе, создание отчетов различных видов и форм: расчет рабочего времени сотрудников, фиксация факта опоздания его на рабочее место и т.д.;

– автоматизированное управление сетью контроллеров объекта: настройка, посылка команд, опрос состояния;

– подключение к пожарно–охранным датчикам и оперативное снятие информации с них;

– объединение контроллеров в независимые группы (подсистемы) для равномерного распределения нагрузки и оптимизации информационных потоков управления.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ, тем, за кого себя выдает. В процедурах идентификации используются различные методы:

– простые, сложные или одноразовые пароли;

– обмен вопросами и ответами с администратором;

– ключи, магнитные карты, значки, жетоны;

– средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук, лица);

– специальные идентификаторы или контрольные суммы для аппаратуры, программ, данных.

Наиболее распространенным методом идентификации является парольная идентификация. Практика показала, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, пароль можно перехватить, а то и просто разгадать. В виду этого, дабы максимально исключить отрицательное влияние человеческого фактора, решено использовать СКУД с проверкой подлинности посредством идентификаторов Touch Memory.

После выполнения процедур идентификации и установления подлинности, пользователь получает доступ в помещение.

В основе большинства средств контроля доступа лежит то или иное представление матрицы доступа.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам защиты от несанкционированных действий. Однако если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации – обнаружить уже совершенные действия или их попытки.

Требования к системе контроля и управления доступом

Все помещения внутри объекта разделяются на три основные зоны по доступности:

– первая зона – помещения, доступ в которые для сотрудников и клиентов не ограничен (например, информационно – справочный зал фирмы, операционный зал банка, пункта обмена валюты, торговый зал универмага, магазина и т.п.);

– вторая зона – помещения, доступ в которые разрешен ограниченному кругу сотрудников (например, отдельные служебные помещения фирм, магазинов, складов и т.п.);

– третья зона – помещения, доступ в которые имеют лишь строго определенные должностные лица объекта (например, кладовые ценностей и сейфовые комнаты банков, ювелирных и оружейных магазинов, кассовые кабины пунктов обмена ваты, помещения подразделений охраны и безопасности, комнаты хранения оружия и т.п.).

СКУД должна состоять из:

– устройств преграждающих управляемых (УПУ) в составе преграждающих конструкций и исполнительных устройств;

– устройств ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;

– устройств управления (УУ), в составе аппаратных и программных средств.

Считывателями и УПУ следует оборудовать:

– главный и служебные входы;

– КПП;

– помещения, в которых непосредственно сосредоточены материальные ценности;

– помещения руководства;

– другие помещения по решению руководства объекта.

Пропуск сотрудников и посетителей на объект через пункты контроля доступа следует осуществлять:

– в здание и в служебные помещения – по одному признаку;

– входы в зоны ограниченного доступа (хранилища ценностей, сейфовые комнаты, комнаты хранения оружия) – не менее чем по двум признакам идентификации.

СКУД должна обеспечивать выполнение следующих основных функций:

– открывание УПУ при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора СКУД;

– запрет открывания УПУ при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;

– санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;

– защиту от несанкционированного доступа к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков;

– защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;

– сохранение настроек и базы данных идентификационных признаков при отключении электропитания;

– ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

– автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;

– выдачу сигнала тревоги (или блокировку УПУ на определенное время) при попытках подбора идентификационных признаков (кода);

– регистрацию и протоколирование текущих и тревожных событий;

– автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с УУ.

УПУ с устройствами исполнительными должно обеспечивать:

– частичное или полное перекрытие проема прохода;

– автоматическое и ручное (в аварийных ситуациях) открывание;

– блокирование человека внутри УПУ (для шлюзов, проходных кабин);

– требуемую пропускную способность.

Считыватели УВИП должно обеспечивать:

– считывание идентификационного признака с идентификаторов;

– сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;

– формирование сигнала на открывание УПУ при идентификации пользователя;

– обмен информацией с УУ.

УВИП должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков.

Выбор конструктивных элементов и физическая реализация системы контроля и управления доступом

СКУД традиционно считаются инструментом обеспечения безопасности. Бесспорно, в настоящее время СКУД – самый эффективный и элегантный способ предотвратить проникновение нежелательных лиц на территорию и в помещения, а своим сотрудникам – обеспечить беспрепятственный проход, но только туда, куда им положено по работе. Но это только часть функций СКУД, притом не самая главная. Кратко основные возможности:

– повышение эффективности работы сотрудников (дисциплина труда, технологическая дисциплина);

– рациональное расходование фонда заработной платы (только за реально отработанное время);

– сокращение штата охранников;

– сокращение трудозатрат на ведение табельного учета, кадрового учета и выдачу пропусков;

– сокращение хищений материальных ценностей и документов;

– сокращение потерь рабочего времени руководителей.

Эти возможности ценны не только сами по себе, но и дают большой экономический эффект. Установка СКУД окупается за 3–5 месяцев, а затем начинает приносить прибыль. Кроме того, система контроля доступа, позволяя современно оформить вход в банк и в помещения, логично завершает общее впечатление от интерьера банка и внешнего вида персонала. Недаром для западных банков и офисов наличие СКУД давно стало корпоративным стандартом, и непременным требованием к ним страховых компаний.

Входы в банк и в служебные помещения оснащаются турникетами, калитками, замками и считывателями карт доступа.

При установке на входе в банк современного турникета–трипода защита от доступа нежелательных или опасных лиц становится гораздо более цивилизованной, чем физическая охрана прохода. Турникет открывается по сигналу от пульта охранника после того, как он переговорит с посетителем и, если необходимо, проверит документы. Сотрудники банка проходят через турникет, предъявляя считывателю идентификатор.

Эти устройства подключаются к контроллерам системы – ее интеллектуальной части, которые объединяются в сеть и подключаются к компьютеру с установленным на нем ПО. Все сотрудники банка получают бесконтактные пластиковые карты доступа. Информация обо всех проходах персонала запоминается и используется для организации учета.

Одним из ведущих предприятий в области разработки и производства приборов разграничение прав доступа является Шлюз Физического доступа Cisco, Cisco Access Gateway, модуль цифровых входов

Планирование IP–адресаций

Для каждого датчика контроля доступа должно быть присвоено свое идентификационное имя, по которому его можно будет определить. Распределение IP адресации для датчиков контроля доступа представлено в таблице 2.3.

Таблица 2.3 – Планирование IP – адресации для разграничения прав доступа

Датчики	IP – адрес/Маска	Шлюз
Cisco Access Gateway	192.168.12.2 – 7/24	192.168.0.1
Модуль цифровых входов	192.168.12.8– 18/24	192.168.0.1
Всего:	15	

Схема построения датчиков контроля доступа 1 и 2 этажа представлена в Приложении Г

Возможности, которые дает установка системы

1 Обеспечение безопасности

– Защита от доступа нежелательных лиц на входе в банк.

При установке на входе в банк современного турникета–трипода защита от доступа нежелательных или опасных лиц становится гораздо более цивилизованной, чем физическая охрана прохода. Турникет открывается по сигналу от пульта охранника после того, как он переговорит с посетителем и, если необходимо, проверит документы. Сотрудники банка проходят через турникет, предъявляя считывателю карту доступа.

Возможно и минимальное решение: установка на входе в банк автономных турникетов или калиток, работающих только под управлением от пульта охранника.

– Защита материальных ценностей и информации.

В реальной жизни сложно добиться, чтобы сотрудники постоянно запирали двери, покидая помещение хотя бы даже на короткое время. Система легко решает проблему сохранности материальных ценностей и документов – покидая помещение, сотрудник просто захлопывает дверь, а, возвращаясь, простым поднесением карты открывает замок.

Кроме того, система позволяет разрешить доступ каждому сотруднику только в те помещения, где он имеет право находиться в соответствии со своими служебными обязанностями.

– Постановка помещений на системную охрану.

Удобство этой функции можно пояснить на простом примере: в бухгалтерию обычно имеют право доступа многие сотрудники, но не в отсутствие хозяев помещения. Поэтому, покидая помещение, сотрудники бухгалтерии могут поставить его на охрану двойным поднесением карты, и, пока кто–либо из них не вернется, сотрудники других отделов не смогут попасть в помещение.

– Проведение служебных расследований**.**

Если возникли проблемы (пропажа ценностей, документов), система легко поможет установить, кто последним входил в помещение, кто ставил или снимал помещение с охраны, – ведь все проходы сотрудников сохраняются в базе данных не только по факту, но и по времени.

– Оперативное управление оборудованием.

Система позволяет следить за всеми событиями в точках прохода и выдает на компьютере оператору или охраннику сообщения о тревожных событиях (взломах замков, нарушениях режима контроля доступа и т.д.). Охранник может оперативно управлять системными устройствами – дистанционно заблокировать замки или, наоборот, открыть их, например, в случае пожара.

2 Контроль трудовой дисциплины и учет рабочего времени

Любой руководитель хочет платить своим сотрудникам за реально отработанное время, а не за опоздания, самовольные отлучки и преждевременные уходы с работы. СКУД, отслеживая все перемещения сотрудников по территории банка, позволяет не только с точностью до минуты учитывать отработанное каждым сотрудником время, но и выявлять все нарушения трудовой дисциплины. Отчеты о нарушителях могут

предоставляться руководству ежедневно, а могут быть просмотрены позже за любой период. При этом немаловажен элемент "безличности" – за дисциплиной следит автоматика, и руководству не приходится брать на себя неприятную роль цербера. Практика установки СКУД показывает, что нарушения трудовой дисциплины сокращаются в 3–4 раза.

Модуль учета рабочего времени позволяет автоматически формировать табель для каждого сотрудника. При этом учитывается только реальное присутствие на рабочем месте – если сотрудник покидал помещение банка в течение дня, время его отсутствия вычитается из общего отработанного времени. Кроме того, время присутствия засчитывается только в рамках индивидуального рабочего графика, поэтому, если сотрудник без производственной необходимости задержался дольше конца рабочего дня, это время не будет проставлено в табель. Вместе с тем, модуль позволяет учитывать время переработки, если она происходит на законных основаниях.

3 Кадровый учет и выдача пропусков

Модули кадрового учета и выдачи пропусков сокращают объем рутинной работы в учетной системе банка. ПО позволяет вносить и сохранять любую информацию о сотрудниках, получать твердые копии учетных карточек, оформлять карты доступа в виде пропуска или бэйджа – с фотографией, ФИО, должностью сотрудника и логотипом банка.

4 Комфортные условия работы руководителей

Руководство банка – самый дорогостоящий его ресурс, и сокращение потерь его времени – "дорогой" вопрос, для которого СКУД предлагает недорогое и удобное решение – пульт руководителя. С помощью этого компактного устройства ответственные лица могут, не вставая из–за стола, управлять дверью своего кабинета – например, закрывать ее на время проведения совещаний или работы с документами. Кроме того, на двери кабинетов может устанавливаться офисный домофон, также работающий на бесконтактных картах.

5 Дополнительный уровень безопасности

– Усиленный контроль доступа в особо важные помещения.

Проход в помещения может быть организован после сеанса видеоконтроля или с применением комиссионирования – по принципу "вход только вдвоем" или "предъявление карты плюс набор секретного кода". Эти функции полностью защищают от попыток воспользоваться чужой картой.

– Мониторинг.

ПО позволяет создавать графические планы банка с реально установленным оборудованием. Кроме того, система позволяет подключать датчики и шлейфы охранно–пожарной сигнализации и анализировать поступающую от них информацию. При возникновении любого тревожного события в ту же секунду оператор системы получит извещение о событии с указанием места на плане, а также инструкцию по действиям в конкретной ситуации.

– Разграничение прав доступа сотрудников по времени и статусу.

Наиболее очевидное применение временных разграничений – запрет доступа в любые помещения банка в нерабочее время (вечером, ночью, в выходные дни), кроме случаев, вызванных служебной необходимостью. Наличие различных статусов пропусков позволяет ранжировать права пользователей системы. Например, руководство банка может пользоваться "генеральными" пропусками, права которых ничем не ограничены; рядовые сотрудники – "стандартными"; а посетители – "временными" с ограниченным сроком действия.

– Защита от передачи пропуска другому лицу.

Обеспечивается функцией Antipassback, которая запрещает повторный проход по одному пропуску без совершения выхода, пресекая попытки провести по своему пропуску кого–либо еще.

6 Объединение в одну систему территориально удаленных объектов

Если банк располагается в нескольких зданиях или имеет филиалы в разных районах города, возможна установка единой СКУД на эти объекты без прокладки кабелей при наличии между ними общей локальной компьютерной сети.

7 Увеличенные системные ресурсы

Используются не только замки и триподы, но также роторные, тумбовые турникеты и калитки. Определим стоимость расширенного решения для уже рассмотренного выше типового комплекта:

Чтобы в полной мере использовать преимущества СКУД, техническому решению должна сопутствовать несложная, но эффективная система организационных мероприятий. Одним из таких обязательных мероприятий является организация матрицы разграничения доступа (таб. 2), в которой приводится соответствие прав доступа субъектов доступа к объектам доступа. В данном случае – это будет означать наличие у сотрудника подразделения прав на вход в помещение. Размерность матрицы определяется количеством субъектов и объектов доступа, по вертикали – субъекты, по горизонтали – объекты. В роли субъектов абстрактно выступают подразделения предприятия, т.к. не имеет смысла составлять матрицу доступа для каждого сотрудника, если можно сузить ее до уровня подразделений (разграничение сотрудников по группам). Условно выделим три типа помещений:

А свободного доступа;

Б ограниченного доступа;

В максимально ограниченного доступа.

К первому типу относятся помещения с номерами 1, 4, 5. Разрешен свободный доступ всем, т.к. здесь происходит взаимодействие с клиентами банка. Доступ во все остальные помещения только для сотрудников банка и сотрудников службы инкассации.

Ко второму типу относятся помещения с номерами 2, 3, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, 23, лестничная клетка. Вход в эти помещения только для сотрудников банка, причем доступ в каждое конкретное помещение для сотрудников разных подразделений различается.

К третьему типу относятся помещения с номерами 6, 7, 8, 9, 14. Помещения максимально ограниченного доступа – не все, а только сотрудники конкретных подразделений имеют право на доступ в эти помещения.

Матрицу разграничений доступа можно просмотреть в таблице 2.4

Таблица 2.4 – Матрица разграничения доступа.

Подразделение	Номер помещения																		
	1	2	3	4-5	6-9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Управляющий	+			+		+	+				+		+			+	+	+	+
Отдел бухгалтерского учета и отчетности	+			+		+	+				+	+	+	+	+		+		+
Отдел по работе с клиентами	+			+		+	+				+		+		+		+		+
Отдел платежных систем	+			+		+					+	+			+	+	+		+
Отдел кредитных операций	+			+							+				+		+		+
Отдел информационных технологий	+			+		+		+	+										
Юридический отдел	+			+							+					+	+		
Отдел анализа и прогнозирования	+			+		+		+				+	+	+	+		+		+
Служба безопасности	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Отдел кадров	+			+		+	+				+		+				+		+
Касса	+			+	+	+				+									
Обменный пункт	+			+	+	+				+									
Архивариус	+			+		+	+	+			+		+						+
Административно–хозяйственный отдел	+			+		+	+				+								

3. Общая сетевая часть предприятия

3.1 Определение структуры потоков данных (размеров и структуры сети).

Сегмент сети – узлы сети, подключенные к одному маршрутизирующему устройству (коммутатор, маршрутизатор) и работающие по одному физическому протоколу.

Широко практикуется разделение сети, основанной на протоколе IP, на логические сегменты, или логические подсети. Для этого каждому сегменту выделяется диапазон адресов, который задается адресом сети и сетевой маской.

Распределение компьютеров между этажами и филиалами:

- Головной офис Алматы:
  - КПП – 1 компьютер;
  - обменный пункт – 1 компьютер;
  - кассы – 3 компьютеров 2 принтера;
  - операционный зал – 4 компьютера;
  - отдел кадров – 2 компьютера;
  - отдел информационных технологий – 2 компьютера;
  - серверная – 3 компьютера;
  - приемная директора– 1 компьютера;
  - управляющий – 1 компьютер;
  - бухгалтерия – 2 компьютера 1 принтер 1 сканер;
  - юридический отдел – 3 компьютеров;
  - отдел анализа и прогнозирования – 6 компьютеров;
  - администрация – 5 компьютеров 1 принтер;
  - отдел кредитных операций – 4 компьютеров;
  - отдел по работе с клиентами – 4 компьютера.

- Филиал Астана №1:
  - кассы –3 компьютера 1 принтер;
  - торговый зал №1 – 6 компьютеров 1 принтер;
  - администрация – 2 компьютера 1 принтер;
  - склад – 2 компьютера;
  - технический отдел – 3 компьютера;
  - бухгалтерия – 2 компьютера 1 принтер.

3.2 Создание логической структуры сети. Разработка информационной структуры предприятия

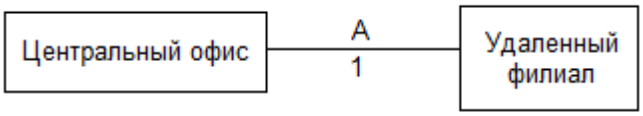
При разработке инфраструктуры предприятия необходимо учесть логическую и физическую структуру предприятия.

Построение логической схемы ЛКС

После информации о потоках данных в сети выполняется сегментирование сети и строится ее логическая схема.

Рекомендуется для каждого представительства организации создавать отдельную ЛКС. Все внешние соединения рассматриваются как соединения с глобальной сетью, а внутренние соединения – с локальной.

Логическую схему необходимо сначала набросать в общем, а затем каждый ее узел описать более детально (Рисунок 3.1).



A – Критически важное соединение.
1 – Соединения с высокой производительностью.

Рисунок 3.1 – Логическая схема сети компьютерной фирмы Логиком

3.3 Выбор топологии сети и методов доступа

При выборе топологии сети необходимо учитывать стоимость сетевого оборудования и его производительность, а также требования предприятия к скорости работы сети.

Из первоначального условия можно сделать однозначный вывод о том, что в конкретном случае не обойтись без комбинированной топологии.

Для анализа первоначальных условий, мы можем прибегнуть к подобию дата логического проектирования. В таком проектировании значимые объекты представляются сущностями, которые могут быть связанны с другими сущностями, либо быть свободными. При этом типы таких связей могут носить разный характер.

В данном случае имеются следующие значимые объекты: рабочее место > кабинет > отдел и здание. Они безусловно должны быть связанными. Принятие решения о том, какую связь выбрать и будет частичным решением поставленной задачи. Исходя из этого, мы можем поставить следующие задачи:

- определение типа связи и топологии ВС в пределах здания;
- определение типа связи и топологии ВС в пределах кабинета.

Поскольку кабинет является наименьшей логической единицей где можно развернуть базовую (элементарную) сеть, то эту сеть можно реализовать на основе одной из базовых сетевых архитектур.

Если посмотреть сводную таблицу оценки значимых критериев и сравнить полученные значения, то безусловным лидером окажется топология «расширенная звезда». Если например полагать, что концентратор будет работать безотказно, то можно прийти к выводу что сеть основанная по подобной топологии окажется самой надежной. Это связанно с тем, что в результате такого вида коммутации, между рабочими станциями образуется

дифференцированная связь «многие ко многим», а это уже в свою очередь самый отказоустойчивый способ объединения (справедливо только при условии, если коммутатор активный и обладает интеллектуальными возможностями). Также связь «многие ко многим» позволяет достичь максимально возможной скорость передачи данных и наилучшего уровня защиты.

Правда еще совсем недавно эта топология не имела столь значительных преимуществ. Связанно это было с отсутствием интеллектуальных концентраторов, которые бы могли в реальном режиме времени управлять трафиком самостоятельно. Поскольку в силу того, что цена на такое оборудование стала доступной даже для домашних пользователей, вспоминать о других способах физического объединения уже не приходиться (разве что изредка они дают о себе знать при применении оптоволоконных технологий, но это отчасти временно и с входом в массы уйдет в забвение).

Определившись с топологией, мы можем приступать к выбору типа связи. Все типы можно условно разделить на две группы: проводную и беспроводную. Поскольку в кабинетах все рабочие места находятся на малом удалении, это дает нам основание пока не рассматривать беспроводную связь в качестве кандидата. Однако если через несколько лет (предположительно) все материнские платы компьютеров будут оснащаться Wi–Fi передатчиками (тоже самое, например, произошло и с usb портами), то необходимость в применении проводной связи все–таки частично снизиться.

Останавливаясь на выборе проводной связи, примем во внимание следующие значимые параметры:

1) скорость передачи;

2) стоимость;

3) готовая инфраструктура.

Теперь необходимо определиться с топологией в масштабах одного отдела (требуется связать кабинеты). В данном случае отлично подойдет топология «звезда» так как, условия объединения остались практически неизменными, т.е. требуется объединить максимально надежным способом различные мало разрозненные сегменты сети. Единственное что изменилось, так это требование к скорости передачи информации. Теперь оборудование должно справляться с многократной нагрузкой.

Также в данном случае можно было бы задействовать топологию «шина». Она обладает хорошей отказоустойчивостью. Если не используется концентратор, то и вероятность выхода из строя сети значительно сокращается. Однако эти плюсы имеют и обратные стороны. Отсутствие концентратора не означает полную отказоустойчивость сети, ведь ее частью также являются и кабели, а разрыв кабеля в сети также может, при определенных обстоятельствах, нарушить всю ее работу. Также без концентратора уменьшается приоритетность и снижается уровень интеллектуального управления трафиком, т.к. всю работу по согласованности потоков информации берут на себя низ лежащие концентраторы (т.е. концентраторы уровня

кабинета), а это не гарантирует отсутствие конфликтов между батареей различных сетевых устройств.

3.4 Планирование IP–адресаций

Для нашей сети целесообразно использовать сети класса С, так как количество компьютеров в сегментах – небольшое. Планирование адресов для головного офиса представлено в таблице 3.1. В таблице 3.2 представлено планирование адресов филиала.

Т а б л и ц а 3.1 – Планирование IP–адресаций головного офиса в Алматы

Отдел	Кол–во комп.	Device	IP–address	Subnet Mask	Default Gateway
Reception	1	PC–1	DHCP 192.168.7.6	/24	192.168.7.1
Бухгалтерия	2	PC–2	DHCP 192.168.8.7	/24	192.168.8.1
		PC–3	DHCP 192.168.8.8	/24	192.168.8.1
Отдел кредитных операций	4	PC–4–7	DHCP 192.168.8.9– DHCP 192.168.8.12	/24	192.168.8.1
Юр. отдел	3	PC–8 –10	DHCP 192.168.8.13 – DHCP 192.168.8.15	/24	192.168.8.1
Отдел информ. технологий	2	PC–11–12	DHCP 192.168.8.16 – DHCP 192.168.8.17	/24	192.168.8.1
Администрация	5	PC–13–17	DHCP 192.168.8.18 – DHCP 192.168.8.22	/24	192.168.8.1
Обменный пункт	2	PC–17–18	DHCP 192.168.9.23– DHCP 192.168.9.24	/24	192.168.9.1
Операционный зал	2	PC–19–20	DHCP 192.168.8.25– DHCP 192.168.8.26	/24	192.168.8.1
Отдел кадров	2	PC–21–22	DHCP 192.168.8.27– DHCP 192.168.8.28	/24	192.168.8.1
Серверная	3	PC–23–25	DHCP 192.168.8.29– DHCP 192.168.8.31	/24	192.168.8.1
Отдел анализа и прогнозирования	6	PC–26–31	DHCP 192.168.8.32– DHCP 192.168.8.37	/24	192.168.8.1
Кассы	3	PC–29 –34	DHCP 192.168.9.38 – DHCP 192.168.9.40	/24	192.168.9.1
Отдел по работе с клиентами	4	PC–35–38	DHCP 192.168.8.41– DHCP 192.168.8.44	/24	192.168.8.1
Приемная директора	2	PC–39	DHCP 192.168.8.45	/24	192.168.8.1
Директор	1	PC–40	DHCP 192.168.8.46	/24	192.168.8.1
	1	Laptop	192.168.8.47	/24	192.168.8.1
Секретарь	1	PC–47	DHCP 192.168.8.49	/24	192.168.8.1
Информационная служба	4	PC–48 – PC–51	DHCP 192.168.8.50 – DHCP 192.168.8.53	/24	192.168.8.1

Таблица 3.2 – Планирование IP–адресаций филиала Астана №1

Отдел	Кол–во комп.	Device	IP–address	Subnet Mask	Default Gateway
Кассы	3	PC–1 – PC–3	DHCP 192.168.11.5 – DHCP 192.168.11.7	/24	192.168.11.1
Торговый зал №1	6	PC–4 – PC–9	DHCP 192.168.11.8 – DHCP 192.168.11.13	/24	192.168.11.1
Администрация	2	Laptop	192.168.11.2	/24	192.168.11.1
		PC–10	192.168.11.4	/24	192.168.11.1
Склад	2	PC–11	DHCP 192.168.11.14	/24	192.168.11.1
		PC–12	DHCP 192.168.11.15	/24	192.168.11.1
Технический отдел	3	Server	192.168.11.3	/24	192.168.11.1
		Router–1 Fa0/0	192.168.11.1	/24	–
		Router–1 Fa0/1	192.168.11.2	/24	–
		PC–13 – PC–15	DHCP 192.168.11.16 – DHCP 192.168.11.18	/24	192.168.11.1
Бухгалтерия	2	PC–16	DHCP 192.168.11.19	/24	192.168.11.1
		PC–17	DHCP 192.168.11.20	/24	192.168.11.1

3.5 Выбор технологии глобальной сети

Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь.

По заданию к курсовой работе указана технология глобальной сети: HPNA.

В 1996 году рядом ведущих производителей телекоммуникационного оборудования был образован альянс, получивший название Home Phoneline Networking Alliance и в 1998 году появился стандарт передачи данных по телефонным линиям, названный HPNA.

Первый версией стандарта является HPNA 1.0, позволяющий передавать данные со скоростью 1 Мбит/сек. Эта версия завоевала популярность и в конце 2000 года была выпущена новая версия, HPNA 2.0, обеспечивающая возможность работы со скоростями 10 Мбит/с при дальности свыше 350м.

Технология HPNA 1.0 (1 Мбит/с) использует метод IEEE 802.3 CSMA/CD (Ethernet) доступа к среде передачи. Полоса пропускания сигнала расположена в пределах от 5,5 МГц до 9.5 МГц, что позволяет не влиять на работу ADSL и VDSL – устройств и телефонов. В HPNA применяется многократная кодировка одиночного битового импульса. Внутри каждого сетевого интерфейса цепь приемника адаптируется к различным уровням помех, которые могут возникнуть в линии. В дополнение к этому, передающая цепь может варьировать уровень сигнала. Принимающая и передающая цепи постоянно контролируют условия прохождения сигнала и подстраивают свои параметры

под эти условия. Именно эта адаптивность позволила существенно снизить требования к среде передачи. По сути, технология HPNA – это мегабитный Ethernet, работающий по телефонным проводам. Это позволяет использовать большое число Ethernet – совместимых программ, драйверов, приложений и оборудования.

Технология HPNA предусматривает использование той же модели драйвера Windows NDIS, который используется существующими картами Ethernet. Работа по принципу Plug–and–Play, поддерживаемая операционными системами Microsoft Windows, полностью освобождает пользователя от необходимости заниматься сложными настройками программного обеспечения.

Большинство существующих абонентских телефонных линий позволяет достичь скорости передачи данных до 100 Мбит/с, при использовании для этого частотного диапазона 2 – 30 МГц. Благодаря использованию новой спектрально эффективной технологии модуляции в HPNA 2.0 обеспечена скорость передачи данных 10 Мбит/с. При этом не только выполняется совместимость оборудования с HPNA 1.0, но и осталась возможность увеличения в будущем скорости передачи до 100 Мбит/с. Новая технология позволяет динамически адаптировать скорость передачи данных и обеспечивает немедленную подстройку в зависимости от изменения электрических характеристик коммуникационного канала.

3.6 Проектирование внешних связей в корпоративной сети

Услуги, связанные с доступом в Internet, предоставляются организациями, которые называются сервис–провайдерами, или поставщиками услуг Internet (Internet service provider, ISP). Сервис–провайдер располагает компьютерной сетью, имеющей постоянное соединение с Internet и включающей в себя компьютеры (серверы доступа), через которые осуществляется подключение абонентов – отдельных пользователей или локальных сетей.

Самым крупным на сегодняшний день провайдером является *«Казахтелеком»* располагающего сегодня самыми значительными ресурсами доступа в Глобальную сеть в Казахстане. Пропускная способность магистральной части сети составляет 622 Мбит/сек. Пропускная способность отдельных локальных сегментов сети достигает 10 Гбит/с. Общая емкость внешних каналов — 965 Мбит/с.

Компания *«Нурсат»* предлагает широкий диапазон возможностей для доступа к сети Интернет в зависимости от потребностей клиента. Для крупного и среднего бизнеса – это подключение по выделенной линии. В качестве выделенной линии используются медная пара, линия ISDN, волоконно–оптическая, либо беспроводная линия связи, на которой организуется цифровой канал связи.

Основные преимущества:

– гибкая тарифная политика;

– широкий диапазон скоростей подключения;

– интернет 24 часа в сутки, 7 дней в неделю с постоянной скоростью передачи данных;

– возможность одновременного использования доступа к сети интернет и телефонной линии;

– возможность подключения существующей локальной сети компании для обеспечения одновременного доступа к сети интернет для нескольких сотрудников компании;

– возможность организации собственной почтовой системы;

– поставка и монтаж необходимого оборудования.

3.7 Выбор сетевых технологий и сетевых протоколов

Внутри ЛКС целесообразно использовать технологию FastEthernet с коммутаторами и концентраторами. Рекомендуется на расстоянии менее 100 м выбирать спецификацию на витой паре категории 5 или 5e (100base–TX– обеспечивает более высокую надежность по сравнению с 100base–T4. Помимо дальности соединения эта спецификация обеспечивает защиту от электромагнитных полей и усложняет возможность несанкционированного подключения к кабелю. Для повышения производительности сети рекомендуется использовать дуплексные связи к серверам и между коммутаторами.

При выборе коммуникационных протоколов следует руководствоваться принципом «чем меньше, тем лучше», поскольку каждый из них создает дополнительный трафик в сети. С помощью общего протокола, который бы подходил для всех служб сети оптимальной конфигурации можно достичь значительного повышения скорости передачи данных. В настоящее время наиболее часто используемым самыми различными службами и платформами стеком протоколов является TCP/IP.

В проектируемой сети будет использоваться интерфейс: FastEthernet 100BaseTX. Интерфейс используется внутри здания, так как протяженность кабеля между хостами не может превышать 100 м, между коммутаторами, между коммутатором и сервером, между коммутаторами и принтерами.

Для коммутации мною был выбран протокол TCP/IP.

3.8 Выбор сетевой операционной системы. Выбор программного обеспечения для защиты информации

Учитывая специфику и профиль предприятия, основной операционной системой пользователей стала Microsoft Windows7 Professional которая является версией ОС для рабочих станций от фирмы Microsoft . Язык интерфейса – английский и русский.

Была выбрана именно эта ОС, так как имеется:

– присоединение к домену и групповые политики;

– подключения к удалённым рабочим столам;
– общий доступ к подключению к интернету;
– быстрое переключение пользователей;
– подключение к беспроводным сетям «на лету»;
– центр мобильности Windows;
– расширенная архивация (сеть и групповые политики);
– печать с учётом местоположения.

Для установки на сервер используем Windows Server 2008 R2

Причины выбора данной ОС:

– устойчивая схема разработки;
– высокая степень документирования системы;
– высокая стабильность системы;
– эталонная схема реализации стека протоколов tcp/ip;
– регулярность обновления и развития системы;
– высокая производительность.

В Windows Server 2008, администраторы могут инсталлировать минимально необходимое окружение для работы определенных ролей. Также это повышает безопасность сервера (уменьшая поверхность атаки), снижает затраты на управление, и требования к ресурсам. Для установки в режиме Server Core Installation на жестком диске достаточно 2Гб свободного места. В ближайшем будущем, во многих компаниях будут стоять двухпроцессорные серверы (4х или 8ми ядерные), с ПО Virtual Server, на которых будет крутиться два–четыре Windows Server 2008 в режиме Server Core Installation, каждый, со своей ролью.

В режиме Server Core Installation можно инсталлировать роли:

– Active Directory Domain Services – Active Directory Lightweight Directory Services (AD LDS) – DHCP Server– DNS Server– File Services– Print Server.

– Для администрации и фильтрации Интернета используем программу UserGate.

Данный набор программ позволяет наладить эффективную работу на автоматизированных рабочих местах, а также обеспечить их безопасность.

На основе этих данных будет построена структура сети (см. Приложение Д).

4. Анализ потенциально опасных и вредных производственных факторов

Опасные и вредные производственные факторы по природе возникновения делятся на следующие группы:

- физические;
- химические;
- психофизиологические;
- биологические.

В помещении лаборатории на программиста могут негативно действовать следующие физические факторы:

- повышенная и пониженная температура воздуха;
- чрезмерная запыленность и загазованность воздуха;
- повышенная и пониженная влажность воздуха;
- недостаточная освещенность рабочего места;
- превышающий допустимые нормы шум;
- повышенный уровень ионизирующего излучения;
- повышенный уровень электромагнитных полей;
- повышенный уровень статического электричества;
- опасность поражения электрическим током;
- блеклость экрана дисплея.

К химически опасным факторам, постоянно действующим на программиста относятся следующие: возникновение, в результате ионизации воздуха при работе компьютера, активных частиц.

Биологические вредные производственные факторы в данном помещении отсутствуют.

К психологически вредным факторам, воздействующим на оператора в течение его рабочей смены можно отнести следующие:

- нервно–эмоциональные перегрузки;
- умственное напряжение;
- перенапряжение зрительного анализатора.

Далее более подробно рассмотрены опасные и вредные факторы, воздействующие на программиста, возникшие в связи с разработкой данной системы.

4.1 Микроклимат рабочей зоны программиста

Микроклимат производственных помещений — это климат внутренней среды этих помещений, который определяется действующими на организм человека сочетаниями температуры, влажности и скорости движения воздуха.

Для создания и автоматического поддержания в лаборатории независимо от наружных условий оптимальных значений температуры, влажности, чистоты

и скорости движения воздуха, в холодное время года используется водяное отопление, в теплое время года применяется кондиционирование воздуха. Кондиционер представляет собой вентиляционную установку, которая с помощью приборов автоматического регулирования поддерживает в помещении заданные параметры воздушной среды.

4.2 Создание оптимальных условий труда

В данном дипломном проекте показан сценарий оборудования отдельного помещения, в котором осуществляются работы с использованием компьютерной техники и электронного оборудования. Помещение, отдела информационных технологий. Главным орудием труда является компьютер и оборудование Cisco, подключенное к нему. В рассматриваемом помещении работают три сотрудника, каждый из которых имеет свое рабочее место. Для сотрудников необходимо создать комфортные условия труда, такие как рабочее место и состояние внутренней среды комнаты, обеспечивающее оптимальную динамику работоспособности, хорошее самочувствие и сохранение их здоровья. Рабочее место обеспечивает возможность удобного выполнения работ в положении сидя. При выборе положения работающего необходимо учитывать физическую тяжесть работ; размеры рабочей зоны и необходимость передвижения в ней работающего в процессе выполнения работ; мероприятия направленные на снижение утомляемости.

Как уже было отмечено, важным моментом организации рабочего места является также определение занимаемой работником площади. Необходимо, чтобы эта площадь позволяла удобно и с наименьшей затратой энергии безопасно и производительно вести трудовой процесс. Примерная планировка помещения показана на рисунке 4.1.

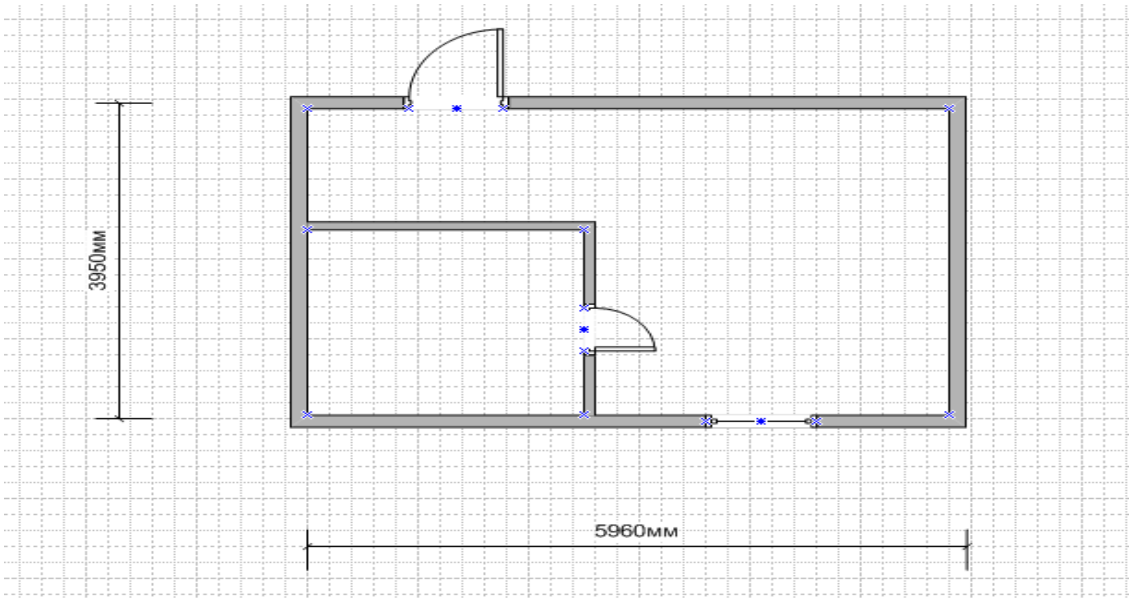


Рисунок 4.1 – Планировка помещения

4.3 Анализ условий труда

Все электротехническое оборудование является потенциальным источником возникновения пожарной опасности. Оборудование малошумящее – вредность в качестве повышенного шума отсутствует. Рабочее помещение, распложенное в здании банка не находится в непосредственной близости от железной дороги или крупной автомагистрали, аэропорта и так далее, поэтому внешних источников шума, влияющих на процесс работы – нет. Повышенный уровень электромагнитных излучений отсутствует (т.к. мы использовали мониторы типа LCD).

Поражение электрическим током может произойти при коротком замыкании, при неумелом обращении с компьютером, при случайном попадании воды на токоведущие части. Для защиты персонала от поражения электрическим током применяют зануление, обеспечивающее быстрое отключение аппарата при замыкании токоведущих частей.

Выполняемая работа относится к категории легких работ (легкая физическая, категория Iа, менее 138 Дж/с, работа производится сидя и не требует физического напряжения), (ГОСТ 12.2.032–78) [31].

Высота рабочей поверхности: 725 мм, высота сиденья: 420мм (ГОСТ 12.2.032–78) , данные ГОСТа указаны в таблице 4.1.

Т а б л и ц а 4 . 1 – Виды работ (ГОСТ 12.2.032–78)

Наименование работ	Класс работ	Высота рабочей поверхности при организации рабочего места	Высота сиденья
Легкие работы	Класс Iа (работа, выполняемая в сидячем положении)	725 *мм*	420 *мм*

Число сотрудников: 3.

Здание: частная организация, расположенное в черте города Алматы. Здание двухэтажное.

Размеры рабочего помещения (комнаты): длина l=6 м, ширина s=4 м, высота h=3 м.

Вид свет пропускающего материала – стекло листовое узорчатое. Вид переплета – стальное двойное открывающееся. Одно окно размером $1\times1{,}5 м^2$.

Искусственное освещение – светильники: люминесцентные лампы ЛД64–4 (4 штуки).

Внутренняя отделка стен – белая.

Режим работы (продолжительность рабочего дня) 9.00 – 18.00.

С перерывом на обед 13.00 – 14.00.

Здание относится к I степени огнестойкости (СНиП РК 2.02–05–2002) [33] данные представлены в таблице 4.2

Т а б л и ц а 4 . 2 – Конструктивная характеристика зданий в зависимости от их степени огнестойкости (СНиП РК 2.02–05–2002)

Степень огнестойкости	Конструктивные характеристики
I	Здания с несущими и ограждающими конструкциями из естественных или искусственных материалов, бетона или железобетона с применением листовых негорючих материалов

Общая площадь помещения 24 м^2. Площадь, занимаемая оборудованием и мебелью 6,8 м^2.

4.4. Пожаробезопасность

Возможность возникновения пожарной ситуации на объектах связи не очень велика. Во всех помещениях установлены ручные углекислотные огнетушители ОУ–5, во дворе здания имеется щит с необходимым для тушения инвентарём.

Все работники каждый год сдают экзамен то технике безопасности, также принимаются дополнительные меры безопасности: плакаты с напоминанием о необходимости осторожного обращения с огнем, выделенные места для курения и т.д.

Так как попадание воды на компьютерную технику, используемую в офисе, может привести к выходу его из строя, то необходимо в данном помещении установить систему противопожарной сигнализации.

В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ–5 с учетом – один огнетушитель на 100м^2. Общая площадь рабочего помещения составляет 24 м^2 таким образом мне необходимо установить один огнетушитель ОУ–5.

На территории здания банка предусматриваются следующие мероприятия для устранения причин пожаров:

– соблюдение противопожарных норм;

– издание необходимых инструкций и плакатов;

– организация экстренного оповещения;

– наличие огнетушителей ОУ–5;

– ограничение или запрещение в пожароопасных местах применения открытого огня, курения, выполнения электрогазосварочных работ.

Организационные мероприятия пожарной профилактики:

– проведение инструктажа 1 раз в год. Производится административно–техническим персоналом;

– разработка путей эвакуации людей при пожаре;

– использование средств тушения и предупреждения пожара (огнетушители, пожарная сигнализация).

Все огнетушители подвергаются периодической проверке и перезарядке. Для предотвращения пожара в начальной стадии предусмотрены следующие средства: внутренний пожарный водопровод, огнетушители ручные, асбестовые одеяла. В коридорах установлены пожарные краны, расположенные в нишах на высоте 1,35м, где также находятся пожарный ствол с напорным рукавом из тканевого материала 10–20м.

При возникновении пожара в производственных помещениях, помимо принятия мер по его ликвидации, необходимо также осуществить эвакуацию из опасной зоны работающего персонала. Эвакуация людей осуществляется по эвакуационным путям, которые должны обеспечивать эвакуацию всех людей, находящихся в помещениях зданий и сооружений, через эвакуационные выходы в течение необходимого времени эвакуации.

По взрывной, взрывопожарной и пожарной опасности производства подразделяются на категории. Помещение бизнес центра относится к категории Е (классификация помещений и зданий по степени взрывопожароопасной ОНТП 24–85) по пожаробезопасности, так как в нём содержатся несгораемые вещества и материалы в холодном состоянии. В таблице 4.3 представлены классификации пожаров.

Таблица 4.3 – Классификация пожаров и рекомендуемые огнегасительные вещества

Классификация пожаров	Характеристика гор. среды, объекта	Огнегасительные средства
А	обычные твердые и горючие материалы (дерево, бумага)	все виды
Б	горючие жидкости, плавящиеся при нагревании материала (мазут, спирты, бензин)	распыленная вода, все виды пены, порошки, составы на основе CO2 и бромэтила
С	горючие газы (водород, ацетилен, углеводороды)	газ. составы, в состав которых входят инертные разбавители (азот, порошки, вода)
Д	металлы и их сплавы (Na, K, Al, Mg)	порошки
Е	электроустановки под напряжением	порошки, двуокись азота, оксид азота, углекислый газ, составы бромэтил+CO^2

4.5 Система вентиляции

Для вентиляции рабочего помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания и открытые окна летом. Однако такая вентиляция не позволяет поддерживать климатические параметры рабочего помещения в пределах нормы (таблица 4.4) в условиях климата города Алматы (в особенности – летом).

Таблица 4.4 – Оптимальные нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно–бытовых помещений (СНиП 2.04.05–91) [34].

Период года	Температура воздуха, ^{0}C	Относительная влажность воздуха, %, не более	Скорость движения воздуха, м/с, не более
Теплый	20 – 22	60 – 40	0,1
Холодный	20 – 22	45 – 30	0,1

Компьютеры, установленные в рабочем помещении, не являются источником выделения тепла (очень незначительное выделение тепла аппаратурой никаким образом не оказывает влияние на микроклимат рабочего помещения).

Климатические условия эксплуатации оборудования полностью совпадают климатическими условиями, нормируемыми для рабочего персонала.

Поскольку климат рабочего помещения не соответствует принятым нормативам, то необходимо для обеспечения нормальных условий микроклимата в помещении оборудовать его дополнительно системой кондиционирования.

В помещении установлен кондиционер: Samsung MH18ZC2 (Рисунок 4.2).

Рисунок 4.2 – Кондиционер Samsung MH18ZC2

Технические характеристики:

- мощность (охлаждение): 5260вт;
- мощность (нагрев): 5560вт;
- потребляемая мощность (охлаждение):890/1780вт;
- потребляемая мощность (обогрев): 870/1740вт;

– питание: 220–240/50(в, гц);
– габариты (внутренний блок): 815×298×182мм;
– габариты (внешний блок): 787×620×320мм;
– пульт управления: есть;
– тип установки: настенный;
– уровень шума: 37/54дб;
– расход воздуха: до 7,5м^3/мин;
– рассчитан на помещение: до 40м^3.

4.6 Разработка мероприятий по улучшению условий труда

4.6.1 Расчет системы кондиционирования

Ниже представлен расчет системы кондиционирования в рабочем помещении. Кондиционирование обеспечит соответствие климата в рабочем помещении нормативам.

Количество приточного воздуха $L_{ПР}$, м^3/ч определяем по формуле:

$$L_{ПР} = \frac{Q_{изб}}{c \times p_{пр} \times (t_{вып} - t_{пр})} \quad (4.1)$$

где $Q_{изб}$ – избыточное выделение явной теплоты,к Дж/ч;

с – удельная теплоемкость воздуха при постоянном давлении, равная с=1кДж/кг·^{0}С;

$p_{пр}$ – плотность поступающего в помещение воздуха, равная 1,2кг/м^3;

$t_{вып}$ – температура удаляемого из помещения воздуха за пределы рабочей или обслуживаемой зоны, ^{0}С;

$t_{пр}$ – температура приточного воздуха, ^{0}С.

Температура удаляемого из помещения воздуха $t_{вып}$, ^{0}С, определяется по формуле:

$$t_{вып} = t_{РЗ} + \Delta t \times (h_{вп} - z) \quad (4.2)$$

где $t_{РЗ}$ – температура в рабочей зоне, которая не должна превышать допустимую по нормам($t_{РЗ} \leq t_{ДОП}$), ^{0}С;

Δt – температурный градиент по высоте помещения (Δt=0,5–1,5), ^{0}С;

$h_{вп}$ – расстояние от пола до центра вытяжных проемов (кондиционера), м;

Н – высота рабочей зоны, м.

Поскольку расчет производится для теплого периода года, то примем $t_{РЗ}$ =22^{0}С.

Внутренняя часть кондиционера расположена на высоте $h_{вп}$=2,5м:

$$t_{вып} = 22 + 1{,}2 \times (2{,}5 - 3) = 21{,}4^0\text{С}.$$

Температура приточного воздуха $t_{пр}$ при наличии избытка явной теплоты должна быть на 5–7^{0}С ниже температуры воздуха в рабочей зоне:

$$t_{пр} = 21{,}4 - 7 = 14{,}4^0\text{С};$$

Величину избыточного выделения явной теплоты $О_{ИЗБ}$ находят на основании баланса теплоты в помещении по формуле:

$$О_{ИЗБ} = \sum Q - \sum Q_{ух} \quad (4.3)$$

где $\sum Q$ – суммарное количество поступающей в помещение явной теплоты;

$\sum Q_{ух}$ – суммарное количество уходящей из помещения теплоты (за счет теплопотерь ограждениями, нагрева поступающего в помещение воздуха и т. п.).

Основными источниками избыточного тепла являются светильники, люди и др. Кроме того, необходимо учитывать теплопоступления от солнечной радиации. В данном помещении тепловыделением электронного оборудования можно пренебречь. Поэтому учитываем тепловыделения от искусственного освещения, от людей, количество тепла, поступающего в помещение через окна от солнечной радиации.

Тепловыделения от искусственного освещения Q_2, рассчитывают, предполагая, что практически вся затрачиваемая энергия, в конечном счете, преобразуется в тепло, по формуле:

$$Q_2 = 1000 \times N \quad (4.4)$$

где N – расходуемая мощность светильников, кВт.

$$Q_2 = 1000 \times 0{,}28 = 280\text{кВт}.$$

Тепловыделения от людей Q_3 определяют по формуле:

$$Q_3 = n \times q_ч \quad (4.5)$$

где n – число работающих;

$q_ч$ – количество тепла, выделяемое одним человеком, Вт (таблица 4.5).

Таблица 4.5 – Количество тепла, выделяемое одним человеком в зависимости от категории работ и температуры окружающей среды

Категория работ	Тепло, $Вт$			
	Полное		Явное	
	при 100^0C	При 350^0C	при 100^0C	При 350^0C
Легкая	180^0C	145^0C	150^0C	5^0C

$$Q_3 = 3 \times 145 = 435\text{Вт}.$$

Количество тепла, поступающего в помещение от солнечной радиации $Q_{ост.рад}$, определяют по формуле:

$$Q_{\text{ост.рад}} = F_{\text{ост}} \times q_{\text{ост}} \times A_{\text{ост}} \quad (4.6)$$

для покрытий:

$$Q_{\text{п.рад}} = F_n \times q_n \times A_n \quad (4.7)$$

где $F_{ост}$ и F_n – площадь поверхности и покрытия, м^2;

$q_{ост}$ и q_n – теплопоступления через 1м^2 поверхности остекления и поверхности покрытия, при коэффициенте теплопередачи, равном Вт/м^2·^{0}С, Вт/м^2;

$A_{ост}$ – коэффициент остекления;

k_n – коэффициент теплопередачи покрытия, Вт/м^2·^{0}С.

Значение $q_{ост}$ в зависимости от географической ориентации поверхности и характеристики окон или фонарей принимается в пределах $70-210$, а коэффициента $A_{ост}$ в зависимости от вида остекления и его солнцезащитных свойств – в пределах 025–1,25, средние значения теплопоступления от солнечной радиации через покрытие в зависимости от географической широты и вида покрытия принимают в пределах 6–24.

$$F_{\text{ост}} = 1{,}5 \times 1 = 1{,}5\text{м}^2;$$

Окно рабочего помещения направлено строго на восток, поэтому примем значение $q_{ост}$ равным 140 Вт/м^2·^{0}С. Примем $A_{ост}$=0,35.

$$Q_{\text{ост.рад}} = 1{,}5 \times 140 \times 0{,}35 = 73{,}5\text{Вт}.$$

Среднее значение теплопоступления для покрытия с учетом географической широты примем равным $Q_{п.рад}$=18Вт.

Потери тепла из помещения $Q_{ух}$, кВт через стены двери, окна оценивают ориентировочно по формуле:

$$Q_{yx} = \frac{\lambda \times S \times (t_{\text{вып}} - t_{\text{пр}})}{\delta} \quad (4.8)$$

где λ – теплопроводность стен, Вт/м·^{0}С;

S – площадь, м^2;

δ – толщина стен, м.

Стены рабочего помещения изготовлены из тяжелого бетона М600, теплопроводность которого равна 1,2 Вт/м·^{0}С. Толщина стен δ =0,5м.

$$Q_{yx} = \frac{1,2 \times 24 \times (21,4 - 14,4)}{0,5} = 403,2\text{Вт}.$$

Вычислим суммарное количество поступающей в помещение явной теплоты:

$$\sum Q = Q_2 + Q_3 + Q_{\text{ост.рад}} + Q_{\text{п.рад}} \quad (4.9)$$

$$\sum Q = 280000 + 435 + 73,5 + 18 = 280526,5\text{Вт}.$$

Вычислим величину избыточного выделения явной теплоты:

$$Q_{\text{ИЗБ}} = 280526,5 - 403,2 = 280123,3\text{Вт}.$$

Вычислим количество приточного воздуха:

$$\text{L}_{\text{ПР}} = \frac{280123,3}{1 \times 1,2 \times (21,4 - 14,4)} = 33348,012\text{м}^3/\text{ч}$$

4.6.2 Расчет искусственного освещения помещения

Рациональное освещение в помещении, предназначенном для работы с ПЭВМ создается при наличии как естественного, так и искусственного освещения.

Недостаточное освещение приводит к сильному напряжению глаз, быстрой утомляемости, близорукости, снижению качества работы, увеличению брака. Яркое освещение раздражает сетчатку глаза, ослепляет, глаза быстро устают, растёт производственный травматизм.

Для создания нормальных условий, на рабочем месте проводят нормирование освещенности в зависимости от размеров объекта различения, контраста объекта с фоном. Определение нормированной освещенности ведется по разрядам и подразрядам выполняемых работ. Для работ, выполняемых разработчикам, отводится четвертый разряд и подразряд “Б”. Минимальное значение нормированной освещенности согласно СНиП 23–05–95 E_{min}=200 Лк для общей системы освещения.

Рассчитаем общее освещение офисного помещения размером 6х4

Нормируемая освещенность – 300 лк.

В помещении принята система общего освещения люминесцентными лампами ЛБ (белого цвета), мощностью 40 Вт и световым потоком Фл = 2900

лм, диаметром 40 мм. и длинной со штырьками 1428,7 мм. Высота рабочей поверхности $h_р$=0,8м.

Индекс помещения, определяется соотношением размеров освещаемого помещения:

$$i = \frac{A \times B}{h(A+B)} \quad (4.10)$$

Определим необходимое расстояние между светильниками:

$$L = \lambda \times h \quad (4.11)$$

где λ=1,5/1,4.

Высота подвеса светильников над рабочей поверхностью:

$$h = H - h_{\text{раб}} = 3 - 0{,}8 = 2{,}2\text{м}.$$

По этим данным находим, что необходимое расстояние между светильниками равно:

$$L = 2{,}2 \times 1{,}4 = 3{,}08 \approx 3\text{м}.$$

Тогда индекс помещения определим, как:

$$i = \frac{6 \times 4}{2{,}2(6+4)} = 0{,}909.$$

В качестве светильника возьмем ЛСП–02 рассчитанный на две лампы мощностью 40 Вт, диаметром 40 мм и длинной со штырьками 1428,7 мм. Световой поток лампы ЛБ 40 Вт составляет 2900 лм., световой поток, излучаемый светильником равен:

$$\Phi_{\text{св}} = \Phi_{\text{л}} \times 2 \quad (4.12)$$

$$\Phi_{\text{св}} = 2900 \times 2 = 5800\text{лм}.$$

Определим число светильников по формуле (27):

$$N = \frac{E \times K_3 \times S \times z}{n \times \Phi_{\text{л}} \times \eta} \quad (4.13)$$

где S – площадь помещения, S= 24 м^2;

K_3 – коэффициент запаса, K_3=1,5$

E– заданная минимальная освещенность, E=300лк;

Z – коэффициент неравномерности освещения, z=1.1/1.2;
n – количество ламп в светильнике, n=2;
$Ф_л$ – световой поток выбранной лампы, $Ф_л$= *3320 лм*;
η – коэффициент использования, η=0,61·

$$N = \frac{300 \times 1{,}5 \times 24 \times 1{,}2}{2 \times 2900 \times 0{,}61} = 3{,}66 \approx 4\text{шт.}$$

Размещаем 2 ряда светильников по 2 светильника в ряду с расстоянием между светильниками в ряду 3 метра. Всего для создания нормируемой освещенности 300 лк необходимо 4 лампы ЛБ мощностью 40 Вт.

Тогда расчетный световой поток будет определяться по формуле:

$$F_р = \frac{E \times K_З \times S \times z}{N \times \eta} \quad (4.14)$$

$$F_р = \frac{300 \times 1{,}5 \times 24 \times 1{,}2}{4 \times 2 \times 0{,}61} = 2655{,}74\text{лм.}$$

Проверка светового потока:

$$\Delta F = \frac{F_л - F_Р}{F_л} \times 100\%; \quad (4.15)$$

$$\Delta F = \frac{2900 - 2655{,}74}{2900} \times 100\% = 0{,}028\%$$

Полученная величина находится в пределах –10%≤ΔF≤+20%, значит перерасчёт светового потока не требуется.

Схема размещения светильников представлена на рисунке 4.3

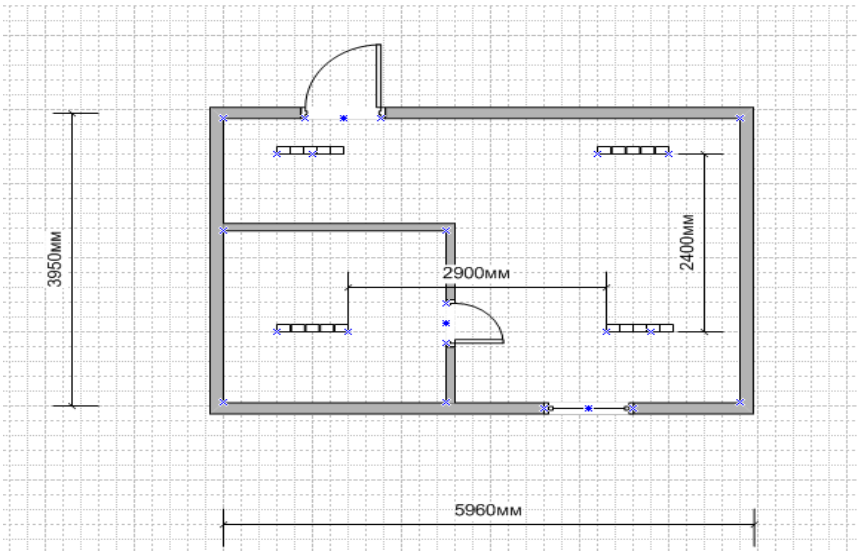


Рисунок 4.3 – Размещение светильников в рабочем помещении

В результате проделанных расчетов просчитаны необходимые меры безопасности и условия труда инженера инфокоммуникационные оборудования, которые соответствуют стандартам СНиП, и ГОСТ.

Произведена необходимая освещенность рабочей поверхности. Выбран тип источника света его светового потока с учетом нормированной освещенности. Рассчитано и показано расположение световых источников.

5. Технико–экономическое обоснование

5.1 Описание работы

Целью данной работы является разработка системы физической безопасности и контроля доступа для здания банка.

Банк создан с целью оказания дополнительной финансовой помощи жителям города Алматы, а так же ведение финансовых дел их клиентов.

Цели банка заключаются не только в получении собственной прибыли, но и увеличение доходов физических лиц с помощью тех же вкладов или получении кредитов на какую–либо покупку. Всё зависит от доходов самого банка, оптимизации его деятельности, рентабельности банка, какие у него доходы, проценты на ссуды, кредиты, ипотеку и т.п. Поэтому для хозяина банка и его служащих целью и будет являться получение большой прибыли, а для частных лиц – увеличение своего дохода, как было сказано через вклады и кредиты.

Основной целью в государстве является стабильная работа банковской деятельности и возможность развития всей экономики в целом, а не отдельных её отраслей. Цели могут быть основаны и на расширении услуг банковской сферы. Она предоставляет своим клиентам больше условий для управления их деньгами, а может увеличить или снизить количество счетов, которые закрываются или понизить, повысить доходы на счетах. Банк также может увеличить доли услуг на рынке. С помощью коммерческих банков можно взять деньги на малый бизнес для каждого человека.

5.2 Программа выполнения работы

Разработка системы безопасности и контроля доступа – сложный и трудоёмкий процесс, требующий наряду с интеллектуальными, техническими затратами и финансовые затраты.

Поскольку работа заключает в себе в основном интеллектуальный труд, необходимо рассчитать затраты на разработку проекта: рассчитать стоимость оборудования, заработную плату персонала, задействованного в разработке, налоги, выплачиваемые в бюджет, накладные расходы и т. д.

Для этого необходимо составить бизнес–план работы в соответствии с утвержденной темой.

Составим бизнес–план по теме «разработка системы физической безопасности и контроля доступа для здания банка», заработную плату каждого работника за час работы и, по каждому наименованию проведённых работ – суммарную заработную плату, а также длительность проведения работ. Далее покажем расчёт амортизационных отчислений на основные средства, расходы на электроэнергию и себестоимость разработки по всем статьям затрат

соответственно, после чего произведем расчет цены интеллектуального труда и оценим затраты на разработку проекта системы защиты периметра сети.

5.3 Расчёт стоимости произведенной работы

Составим смету затрат на разработку проекта системы защиты периметра компьютерной сети.

Смета затрат, произведенных при разработке проекта состоит из основных, накладных и прочих затрат. Основные затраты состоят из: расходов на материалы, зарплату производственного персонала, налоги, выплачиваемые в бюджет. К накладным расходам относятся транспортные расходы, зарплата вспомогательного персонала, налоги и т.д. Прочие расходы: расходы на канцелярские товары, связь, коммунальные услуги и т.д.

Рассчитаем капитальные вложения на внедрение проекта. Капитальные вложения включают в себя стоимость оборудования, монтажные работы, транспортные вложения и прочие расходы.

Общие капитальные вложения вычисляются по формуле:

$$\Sigma К = К_о + К_м + К_{тр} + К_{пр} \quad (5.1)$$

где $К_о$ – капитальные вложения на приобретение оборудования;

$К_м$ – капитальные вложения на монтажные работы;

$К_{тр}$ – капитальные вложения на транспортные расходы (5–10% от стоимости оборудования);

$К_{пр}$ – прочие капитальные вложения.

Перечень необходимого оборудования и общая сумма капитальных вложений на оборудование представлено в таблице 5.1

Таблица 5.1 – Смета капитальных вложений на приобретение оборудования

Наименование оборудования	Количество	Цена за единицу, тенге	Сумма, тенге
Дымовой пожарный из вещатель sc460	37	2 347	86 839
Приемно–контрольный прибор sc470	18	2 740	49 320
Датчик влажности sc510	5	2 458	12 290
Беспроводная видеокамера Cisco 2500W	6	8 960	53 760
Купольная IP камера 5010,5011	29	7 500	217 500
Коммутатор Cisco 2960	1	240 000	240 000
Маршрутизатор Cisco 800/3600	1	200 000	200 000
Шлюз контроля доступа Cisco	6	9 800	58 800
Модуль цифровых входов	11	5 800	63 800
Итого			982 309

Капитальные вложения на монтаж оборудования составляет 354 000 тенге (см. таблицу 5.2)

Таблица 5.2 – Смета капитальных вложений на монтажные работы

Наименование оборудования	Количество	Цена на установку единицы, тенге	Сумма, тенге
Дымовой пожарный из вещатель sc460	37	1700	62 900
Приемно–контрольный прибор sc470	18	1 500	27 000
Датчик влажности sc510	5	1 200	6 000
Беспроводная видеокамера Cisco 2500W	6	6 000	36 000
Купольная IP камера 5010,5011	29	5 000	145 000
Коммутатор Cisco 2960	1	11 000	11 000
Маршрутизатор Cisco 800/3600	1	10 000	10 000
Шлюз контроля доступа Cisco	6	4 500	27 000
Модуль цифровых входов	11	2 700	29 700
Итого			354 600

При любой деятельности возникают транспортные расходы, которые составляют 5–10% от стоимости оборудования. Расчет капитальных транспортных расходов подсчитаем по высокой ставке.

$$К_{тр} = 982\,309 \times 10\% = 98\,230{,}9 \text{ тенге.}$$

Так же при установке оборудования использовали унифицированный кабель, подходящий для всех устройств. Было затрачено 180 метров данного кабеля общей стоимостью 16 200 тенге.

Таким образом, общая сумма капитальных вложений составляет:

$$\Sigma К = 982\,309 + 354\,600 + 98\,230{,}9 + 16\,200 = 1\,451\,339{,}9 \text{ тенге.}$$

5.4 Эксплуатационные расходы

Текущие затраты на эксплуатацию определяются по формуле:

$$Э_р = ФОТ + О_С + А_О + Э + Н \qquad (5.2)$$

где ФОТ – фонд оплаты труда;

$О_С$ – отчисления на соц. нужды;

$А_О$ – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

Н – накладные затраты.

Фонд оплаты труда

В штате состоят 2 – инженера–техника, 1 – начальник отдела. Месячная зарплата у каждого инженера–техника составляет 100 000 тенге. Месячная зарплата у начальника отдела составляет 150 000 тенге. Заработная плата сотрудников приведена в таблице 5.3

Т а б л и ц а 5 . 3 – Заработная плата сотрудников

Исполнитель	Количество человек	Заработная плата за месяц	Общая сумма в месяц	Заработная плата в год
Начальник отдела	1	150 000	150 000	1 800 000
Инженер–техник	2	100 000	200 000	2 400 000
Итого	3		350 000	4 200 000

Затраты по оплате труда состоят из основной и дополнительной заработных плат и рассчитываются по формуле:

$$ФОТ = З_{осн} + З_{доп} \quad (5.3)$$

где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата.

Основная заработная плата ($З_{осн}$) в год составляет 4 200 000 тенге.

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле:

$$З_{доп} = 0{,}1 * З_{осн} \quad (5.4)$$

$З_{доп} = 0{,}1 * 4\ 200\ 000 = 420\ 000$ тенге.

Общий фонд оплаты труда за год составит:

$ФОТ = 4\ 200\ 000 + 420\ 000 = 4\ 620\ 000$ тенге.

Расчет затрат по социальному налогу

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле:

$$О_С = 0{,}11 \times (ФОТ - ПО) \quad (5.5)$$

где ПО – отчисления в пенсионный фонд;

ФОТ – фонд оплаты труда;

0,11 – ставка на социальные нужды.

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле:

$$ПО = 0{,}1 \times ФОТ \quad (5.6)$$

$$ПО = 0{,}1 \times 4\,620\,000 = 462\,000 \text{ тенге.}$$

Тогда социальный налог будет равен:

$$О_С = 0{,}11 \times (4\,620\,000 - 462\,000) = 457\,380 \text{тенге.}$$

Расчет затрат на амортизацию

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 25% и вычисляются по следующей формуле:

$$А_о = Н_А \times \sum К \quad (5.7)$$

где $Н_А$ – норма амортизации;

$\sum К$ – стоимость оборудования.

Тогда амортизационные отчисления составляют:

$$А_о = 0{,}25 \times 1\,451\,339{,}9 = 362\,834{,}98 \text{ тенге.}$$

Расчет затрат на электроэнергию

Затраты на электроэнергию для производственных нужд в течение года, включают в себя расходы электроэнергии на оборудование и дополнительные нужды и рассчитываются по формуле:

$$Э = З_{эл.обор} + З_{доп.нуж} \quad (5.8)$$

где $З_{эл.обор}$ – затраты на электроэнергию для оборудования;

$З_{доп.нуж}$ – затраты на дополнительные нужды.

Затраты электроэнергии на оборудование рассчитывается по формуле

$$З_{эл.обор} = W \times T \times S \quad (5.9)$$

где W – потребляемая мощность, W=7кВт;

T – время работы (на 2014 год при шести дневной 40 часовой рабочей составляет 1983часа);

S – тариф, равный 1 кВтч = 14,65 тенге.

$$З_{эл.обор} = 5 \times 14{,}65 \times 1983 = 145\ 254{,}75 \text{тенге.}$$

Затраты на дополнительные нужды составляют 5% от затрат на электроэнергию оборудования и рассчитываются по формуле:

$$З_{доп.нуж} = 0{,}05 \times З_{эл.обор} \quad (5.10)$$

где $З_{эл.обор}$ – затраты на электроэнергию для оборудования;

Затраты на электроэнергию для дополнительных нужд:

$$З_{доп.нуж} = 0{,}05 \times 145\ 254{,}75 = 7\ 262{,}74 \text{ тенге.}$$

Тогда суммарные затраты на электроэнергию будут равны:

$$Э = 145\ 254{,}75 + 7\ 262{,}74 = 152\ 517{,}49 \text{тенге.}$$

Расчет накладных затрат

Накладные расходы составляют 30% от всех затрат и рассчитываются по формуле:

$$Н = 0{,}5 \times (ФОТ + О_С + А_О + З_{эл.обор}) \quad (5.11)$$

Тогда накладные затраты составят:

$$Н = 0{,}5 \times (4\ 620\ 000 + 457\ 380 + 362\ 834{,}98 + 152\ 517{,}49) =$$
$$= 2\ 796\ 366{,}23 \text{ тенге.}$$

5.5 Оценка экономической эффективности от реализации проекта

В настоящее время отсутствуют единые директивно установленные нормативы эффективности. Коэффициент эффективности рассчитывается по формуле:

$$Е = \frac{П}{К} \quad (5.12)$$

где: Е – коэффициент общей экономической эффективности;

П – прибыль;

К – общие капитальные вложения.

Прибыль рассчитывается по формуле:

$$П = Д - И \quad (5.13)$$

где: П – прибыль;

Д – доход;

И – издержки.

В качестве дохода мы рассматриваем предполагаемый ущерб, который может понести банк в случае отсутствия данной системы защиты и который составляет 3 159 200 тенге.

Таким образом, прибыль составит:

$$П = 3\,159\,200 + 2\,796\,366{,}23 = 362\,834 \text{ тенге.}$$

Таким образом, коэффициент абсолютной экономической эффективности от реализации проекта составит:

$$Е = \frac{362\,834}{1\,451\,336} = 0{,}25.$$

Срок окупаемости проекта рассчитывается по формуле:

$$Т = \frac{1}{Е} \qquad (5.14)$$

И составит:

$$Т = \frac{1}{0{,}25} = 4 \text{ года.} \qquad (5.15)$$

Сводные результаты расчета экономической эффективности от реализации проекта представлены в таблице 5. 4.

Т а б л и ц а 5 . 4 – Результаты расчета экономической эффективности

Показатель	Сумма
Кап. Вложения (Кв),тенге	1 451 339,90
Эксплуатационные издержки (Э), тенге	2 796 366,23
Прибыль (П), тенге	362 834
Коэффициент экономической эффективности (Е)	0,25
Срок окупаемости проекта (Т),лет	4

Заключение

В рамках дипломного проекта:

- проведен анализ объекта информатизации и разработана нормативная документация по объекту;
- разработана модель потенциального нарушителя;
- сформулированы требования к проектируемой системе и составлено техническое задание на разработку системы физической защиты;
- исследован рынок и произведен выбор средств инженерно–технической защиты;
- построен сетевой график и определена технология проведения работ;
- сформулированы необходимые организационно–экономические мероприятия;
- подготовлена необходимая техническая документация;
- выполнен и обоснован экономический анализ;
- проведен анализ условий труда оператора ЭВМ.

Спроектированная система имеет высокий технический уровень. Очевидными достоинствами являются: удобство пользования для сотрудников; удобство администрирования; расширенные функциональные возможности; гарантийные условия.

Представленная система универсальна, а за счет того, что состоит из многих однотипных элементов – легко модифицируема и надежна. После внедрения системы суммарный риск появления угрозы снизится более чем в два раза.

Рассмотренные в данном проекте теоретические вопросы обеспечения физической безопасности и практические вопросы проектирования позволяют сформировать необходимые знания и навыки для решения на практике таких задач как: формулирование концептуальных положений организационного обеспечения информационной безопасности предприятия; организация службы безопасности объекта; профотбор и работа с кадрами; организация внутри объектового режима и охраны объектов; разработка и проектирование интегрированных систем физической охраны на объекте; экономическое обоснование целесообразности создания комплексной системы защиты на предприятии.

Тем самым достигнута основная цель всей работы – проектирование интегрированной системы физической охраны объекта информатизации

Список сокращений

1 АКБ – акционерный коммерческий банк
2 АУПТ – автоматическая установка пожаротушения
3 АУПС – автоматическая установка пожарной сигнализации
4 БД – база данных
5 ИСБ – интегрированная система безопасности
6 ИТЗ – инженерно–техническая защита
7 ИТС – инженерно–технические средства
8 КБ – коммерческий банк
9 КПП – контрольно–пропускной пункт
10 ЛВС – локальная вычислительная сеть
11 МВД – министерство внутренних дел
12 НСД – несанкционированный доступ
13 НТД – нормативно–техническая документация
14 ОПС – охранно–пожарная сигнализация
15 ПКП – приемно–контрольный прибор
16 ПКПП – приемно–контрольный прибор пожарный
17 ПКПО – приемно–контрольный прибор охранный
18 ПКПОП – приемно–контрольный прибор охранно–пожарный
19 ПО – программное обеспечение
20 ПС – программные средства
21 ПСО – периметральная система охраны
22 ПЭВМ – персональная электронно–вычислительная машина
23 ПЭМИН – побочные электромагнитные излучения и наводки
24 СБ – служба безопасности
25 СВТ – средства вычислительной техники
26 СКУД – система контроля и управления доступом
27 СОТ – система охранного телевидения
28 СОУЭ – система оповещения и управления эвакуацией
29 СФЗ – система физической защиты
30 ТЗ – техническое задание
31 ТС – тревожная сигнализация
32 ТСВ – телевизионная система видеоконтроля
33 ТСО – технические средства охраны
34 ТС – технические средства
35 УВИП – устройств ввода идентификационных признаков
36 УПУ – устройство преграждающее управляемое
37 УУ – устройство управления
38 ЧС – чрезвычайная ситуация
39 ЧТЗ – частное техническое задание
40 ШС – шлейф сигнализации
41 ЭВМ – электронно–вычислительная машина
42 ЭВТ – электронно–вычислительная техника
43 DHCP – Dynamic Host Configuration Protocol

44 FTP – File Transfer Protocol
45 HTTP – HyperText Transfer Protocol
46 IT – Information Technologies
47 IEEE – Institute of Electrical and Electronics Engineers
48 IGMP – Internet Group Management Protocol
49 IP – Internet Protocol
50 LAN – Local Area Network
51 MPEG – Moving Picture Experts Group
52 QoS – Quality of Service
53 OSI – Open Systems Interconnection
54 PoE – Power over Ethernet
55 RJ–Registered Jack
56 RTP – Real–time Transport Protocol
57 SAP – Security Association Protocol
58 SNMP – Simple Network Management Protocol
59 TCP/IP – Transmission Control Protocol / Internet Protocol
60 VLAN – Virtual Local Area Network
61 WAN – Wide Area Network
62 VSM –Video Surveillance Manager

Условно графические обозначения

– Шлюз контроля доступа

– Шлюз контроля доступа с клавиатурой

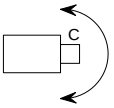

– Турникет

– Датчик движения, вибрации, температуры Cisco sc 470

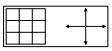
– Датчик дыма Cisco sc 460

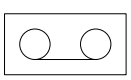

– Датчик влажности Cisco sc 510.

– Купольная камера Video Surveillance 5010



– Уличная камера Video Surveillance 2500W


– Видео стена Virtual Matrix



– Записывающие устройство multiservices платформа 1–RU


– Медиа–сервер видеонаблюдения

Список литературы

1 Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности. 2001, – № 41. – С. 93.

2 Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М.: 2001. – 496 с.

3 Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.

4 Галатенко В.А. Стандарты информационной безопасности / Под редакцией академика РАН В.Б. Бетелина // – М.: ИНТУИТ.РУ «Интернет–университет информационных технологий», 2004.

5 Долин П.А. Справочник по технике безопасности. – 6–е изд., перераб. и доп. – М.: Энергоатомиздат, 1984. – 824 с.

6 Каменев П.Н. Отопление и вентиляция. Часть II Вентиляция. – М.: Издательство литературы по строительству, 1976. – 439 с.

7 Дзюндзюк Б.В., Иванов В.Г., Клименко В.Н., Солдатов А.В., Стыценко Т.Е.,Тулупов С.Д., Филипенко И.А. Учебное пособие. – Харьков: Харьковский национальный университет радиоэлектроники, 2006. – 244с.

8 НПБ 88–2001. Нормы пожарной безопасности. Установки пожаротушения и сигнализации. Нормы и правила проектирования. – М.: Издательство стандартов, 2001.

9 Охрана труда на предприятиях связи и охрана окружающей среды: Учебник для вузов / Н. И. Баклашов, Н. Ж. Китаева, Б. Д. Терехов. – М.: Радио и связь, 1989. – 288 с., ил.

10 Балашов П.А. Некоторые аспекты оснащения объекта средствами безопасности. – Конфидент, 2000. –№2. –С. 80–91.

11 Башин А.В. Видеонаблюдение как часть интегрированной системы безопасности. – Конфидент, 1997. –№6. –С. 55–59

12 Вишняков С.М. Системы комплексной безопасности: вопросы стандартизации. – Конфидент, 2002. – №1. – С. 32–35.

13 Зайцев А. Четыре важных момента. Особенности применения приемно−контрольных приборов охранной сигнализации большой информационной емкости. – Конфидент, 2002. –№ 4. –С. 150–152.

14 Калашников С.А., Тевдорашвили А.В. Приборы противопожарной автоматики ООО «Сталт». – Конфидент, 2001. – №1. – С. 31–34.

15 Козьминых С.И. Интегрированные системы безопасности фирмы «Сигма–ИС». – Конфидент, 2002. – №1. – С. 61–63.

16 Козьминых С.И., Забияко С.В. Методологические принципы проектирования интегрированных систем безопасности. – Конфидент, 2002. – №1. – С. 35–40.

17 Крошкин А.Н. Проектная документация для интегрированных систем безопасности – Конфидент, 2003. –№5. –С. 80–91.

18 Крошкин А.Н. Техническое задание на создание интегрированной системы безопасности объекта – Конфидент, 2003. –№3. –С. 92–96.

19 Крылов В.М., Левин Ю.М. Alpha и Omega интегрированных систем безопасности – Конфидент, 2002. –№1. –С. 51–54.

20 Курило А.П. О защите банковской тайны – Конфидент, 2001. –№3. –С. 18–23.

21 Новейшие российские технологии в системах охранно–пожарной сигнализации – Конфидент, 2001. –№1. –С. 22–24.

22 Новицкий А.П. «Новые информационные технологии в системах видеонаблюдения» – Конфидент, 1999. –№4–5. –С. 108–111.

23 Новицкий А.П. «Компьютерные системы наблюдения: устройство и эксплуатация» – Конфидент, 2000. –№4–5. –С. 82–85.

24 Омельянчук А.М. Интегрированные системы масштаба объекта – Конфидент, 2002. –№1. –С. 49–51.

25 Панюков Д.В. Как защитить завод – Конфидент, 2002. –№1. –С. 40–43.

26 Сидорчук Р.Ю. Несколько советов по защите периметров – Конфидент, 2001. –№1. –С. 18–21.

27 Сичко Ж.В., Козлова О.Л., Соколова Е.Ю., Чубенко А.Е. Профилактика нарушений в состоянии здоровья у работающих с видеотерминалами: Методические материалы докладов Российской научно–практической конференции "Комплексные мероприятия по охране труда, пожарной безопасности и укреплению здоровья работников при различных видах трудовой деятельности". 16–17 апреля 1997, – С. 131–133.

28 З.Д. Еркешева, Г.Ш. Боканова. Методические указания к выполнению семестровых работ для студентов специальности 5В070400 – «Вычислительная техника и программное обеспечение». – Алматы: АУЭС, 2013

29 Брусакова И.А., Чертовской В.Д. Информационные системы и технологии в экономике. – М.: Финансы и статистика, 2007. – 352 с.

30 ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования. - М.: Издательство стандартов, 1978.

31 СНиП РК 2.04-05-2002 Естественное и искусственное освещение строительные нормы и правила. - А.: Издательство стандартов, 2002.

32 СНиП РК 2.02-05-2002 Пожарная безопасность зданий и сооружений. - А.: Издательство стандартов, 2002.

33 СНиП РК 2.04.05-91 Отопление, вентиляция и кондиционирование. - А.: Издательство стандартов, 1991.

34 СНиП РК 2.23–05–95 Минимальное значение нормированной освещенности. - А.: Издательство стандартов, 2003.

35 Голубицкая Е.А. Экономика связи. – М.: Ирмас, 2006.

36 Сайт http://studlib.com/content/view/1675/25/

37 Сайт http://kiev–security.org.ua/b/22/7.shtml

38 Сайт http://daily.sec.ru/

39 Сайт http://www.oskord.ru/ru/News/Message/460QK6A.html
40 Сайт http://www.fbgroup.ru/index.php
41 Сайт http://www.f–sb.ru/
42 Сайт http://www.kiev–security.org.ua
43 Сайт http://obzor.emit–group.ru/?id=10307
44 Сайт http://www.bre.ru/security/83.html
45 Сайт http://www.cisco.com/web/RU/index.html
46 Сайт http://bolid.ru/
47 Сайт http://www.itrade–group.ru/
48 Сайт http://www.open–security.org/solaris/
49 Сайт http://daily.sec.ru/2005/03/14/N–SHumilov–Nauchno–metodicheskoe–soprovoshdenie–sozdaniya–sistem–fizicheskoy–zashiti–obektov.html
50 Сайт http://www.metal–rofi.ru/library/economy/kontceptcij_banka.htm
51 Сайт http://window.edu.ru/resource/425/55425
52 Сайт http://www.crime–research.ru/library/security7.htm
53 Сайт http://e.lib.vlsu.ru/
54 Сайт http://www.studmed.ru/
55 Сайт http://lib.znate.ru/docs/index–159212.html
56 Сайт http://daily.sec.ru/%&Ovr0/dailypblshow.cfm?rid=12&pid=6881&pos=3&stp=10

Приложение А

Схема помещений 1 и 2 этажей здания банка представлена на рисунках А1 и А2.

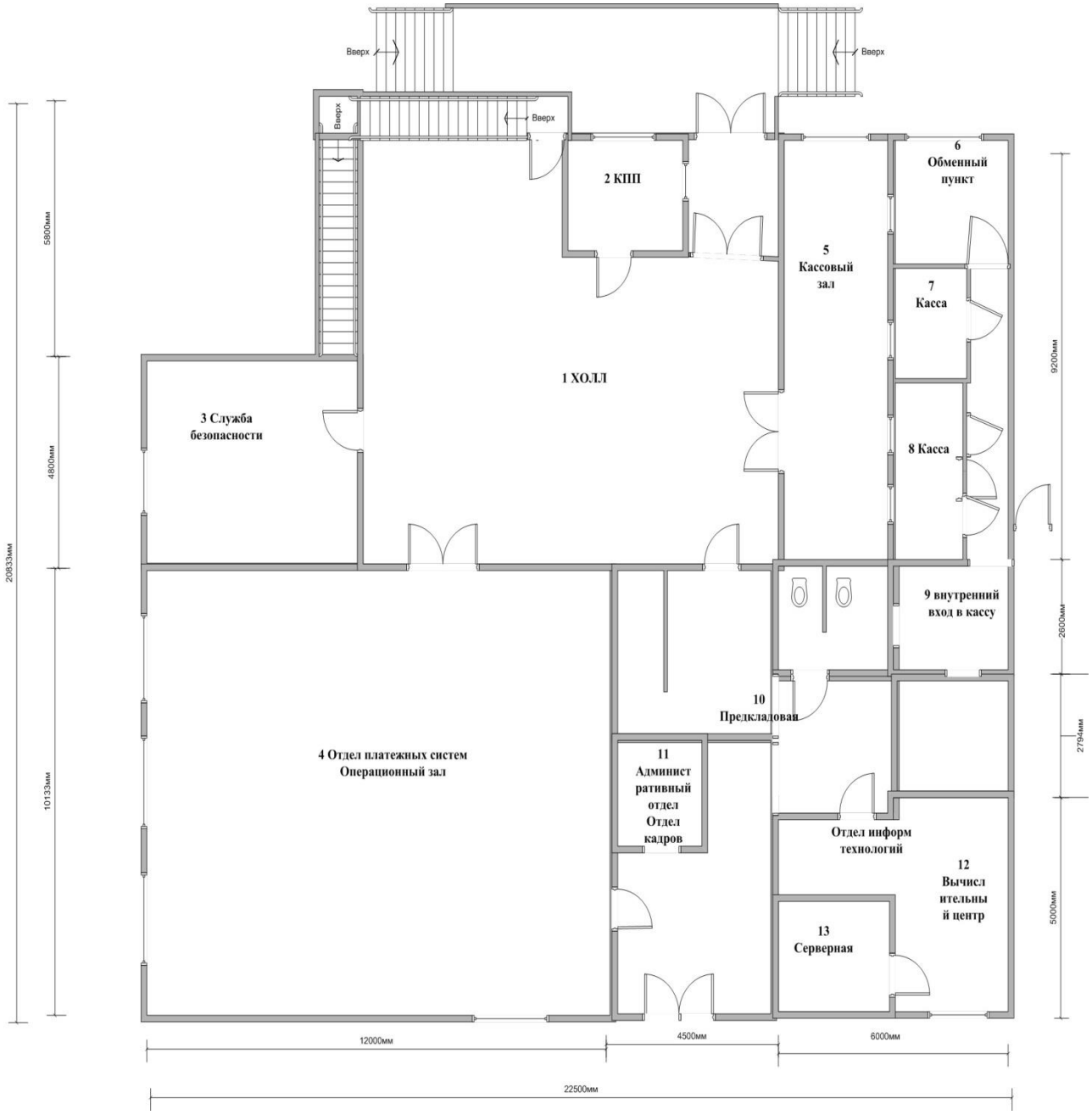


Рисунок А1 – Расположение и номера помещений первого этажа

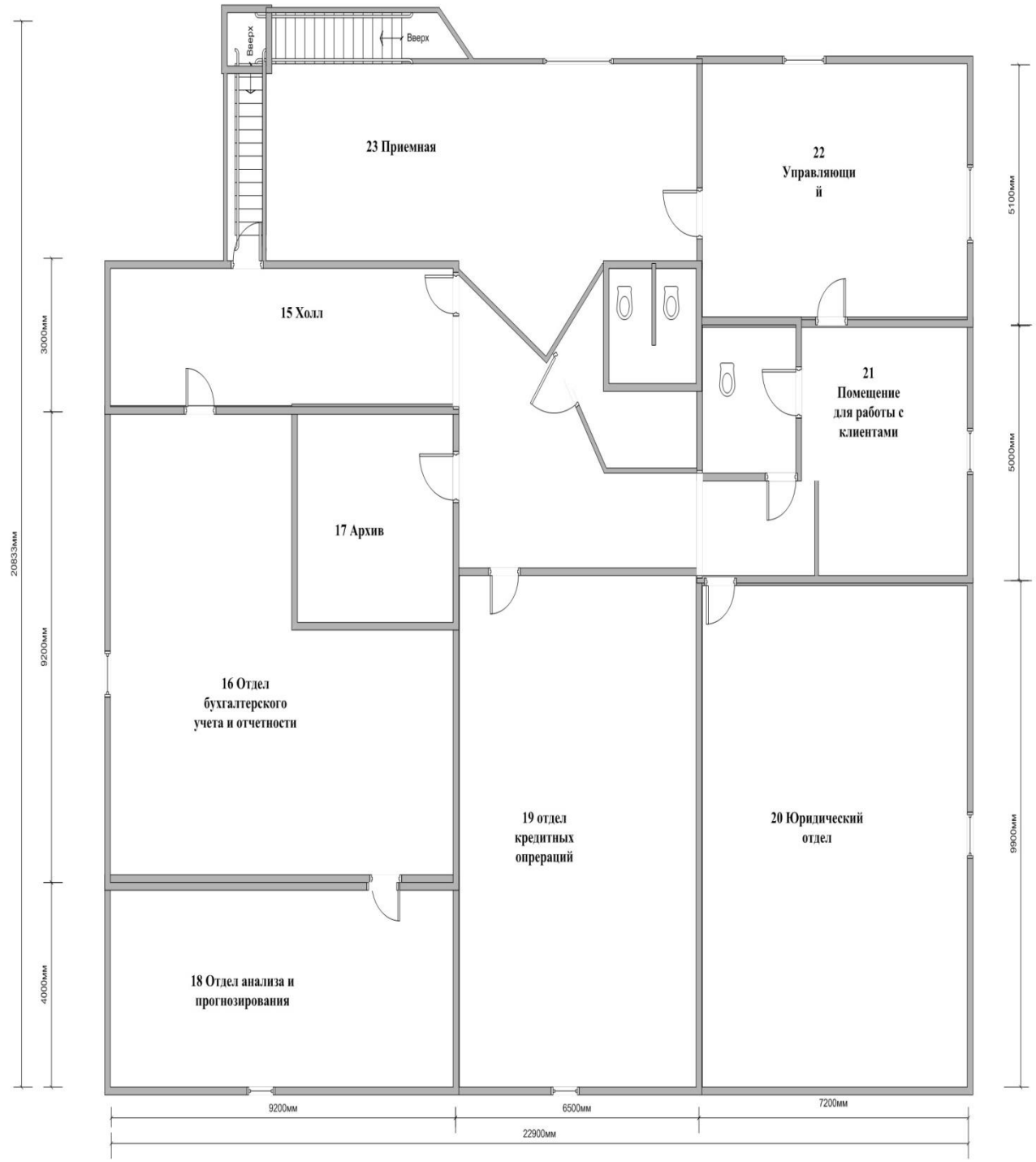


Рисунок А2 – Расположение и номера помещений второго этажа

Приложение Б

Схема расположений пожарных из вещателей представлена на рисунках Б1 и Б2.

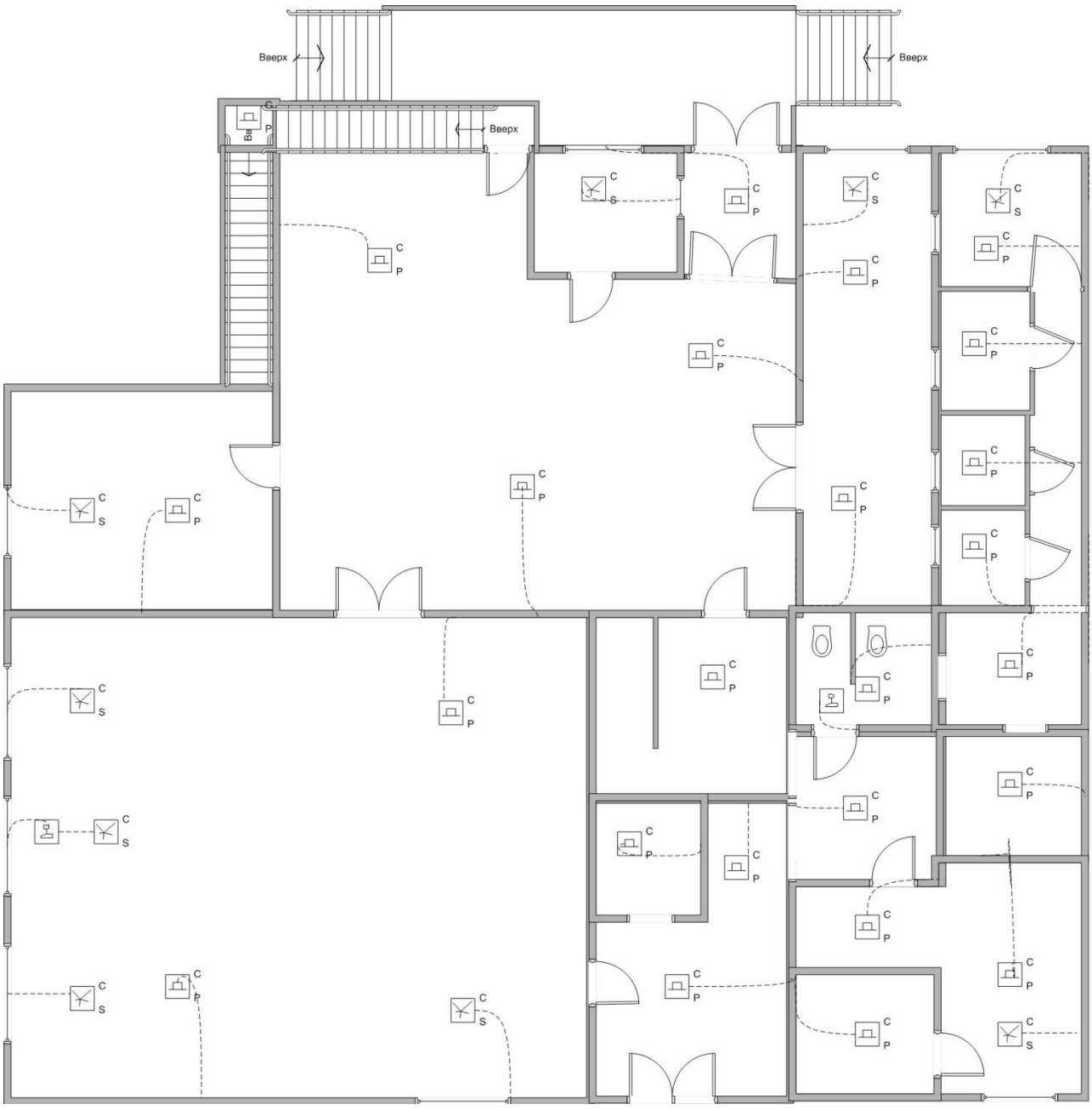


Рисунок Б1 – Расположение пожарных из вещателей на первом этаже

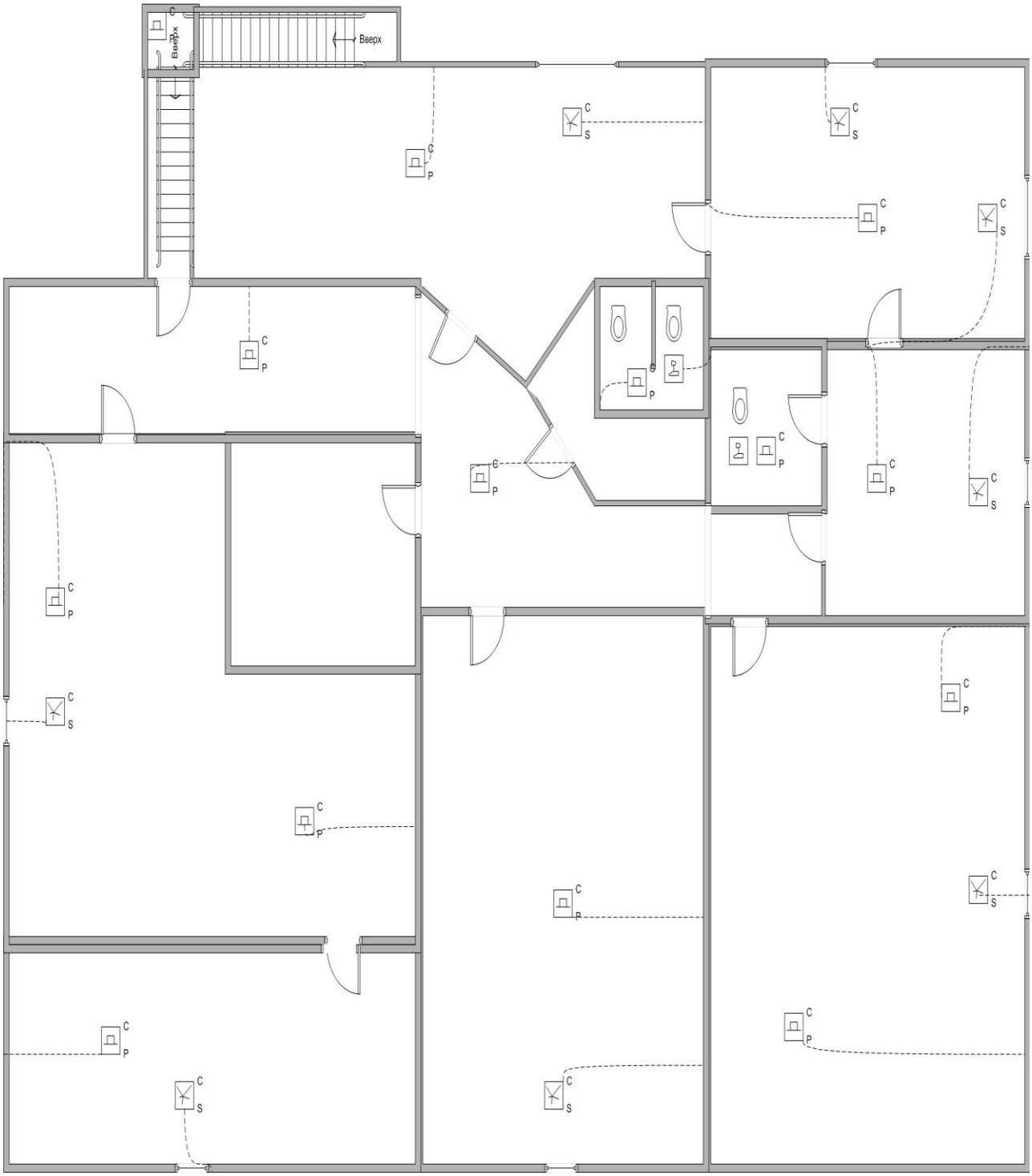


Рисунок Б2 – Расположение пожарных из вещателей на втором этаже

Приложение В

Схема расположений камер видеонаблюдения представлена на рисунке В1 и В2.

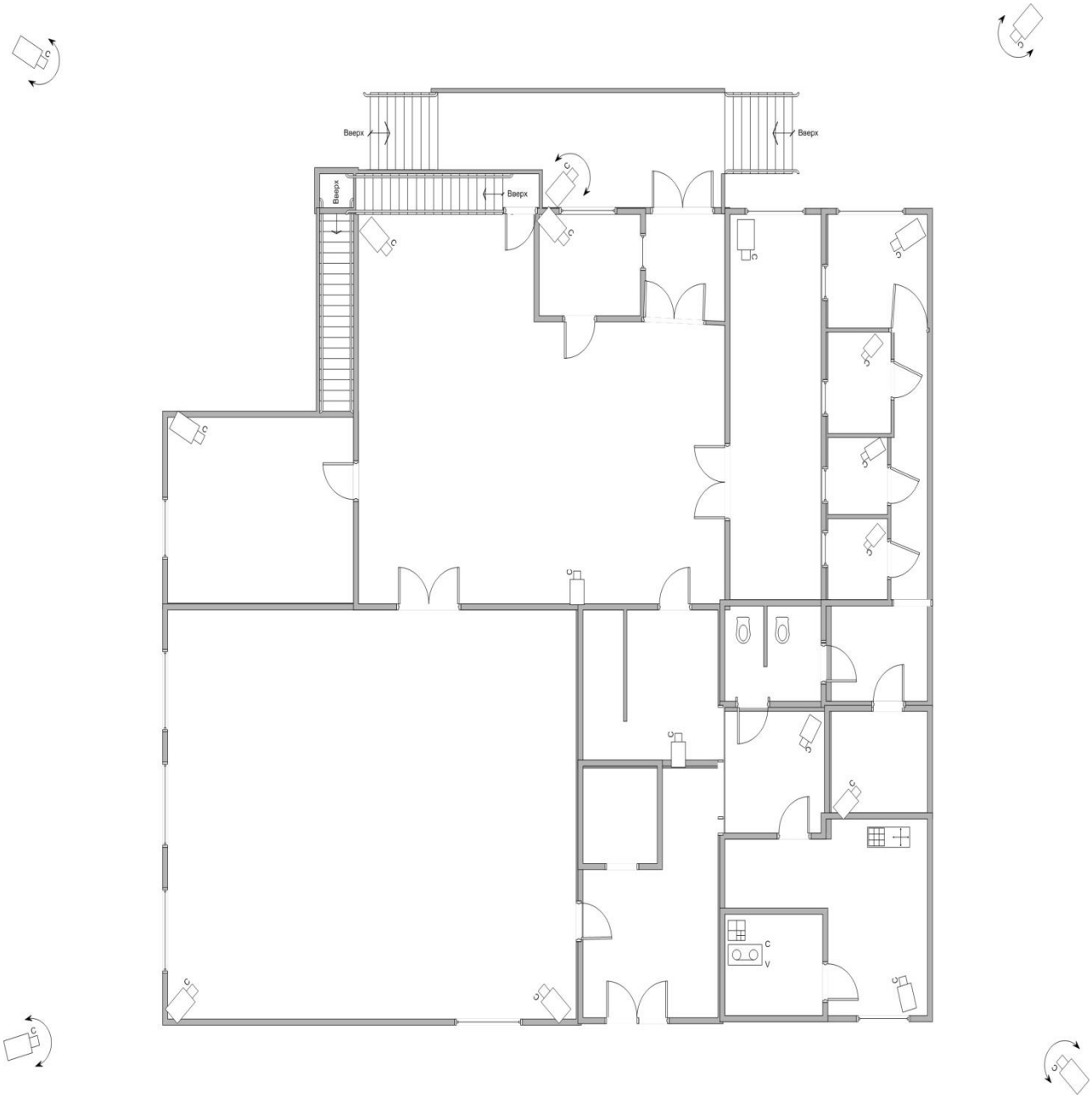


Рисунок В1 – Расположение элементов системы видеоконтроля первого этажа

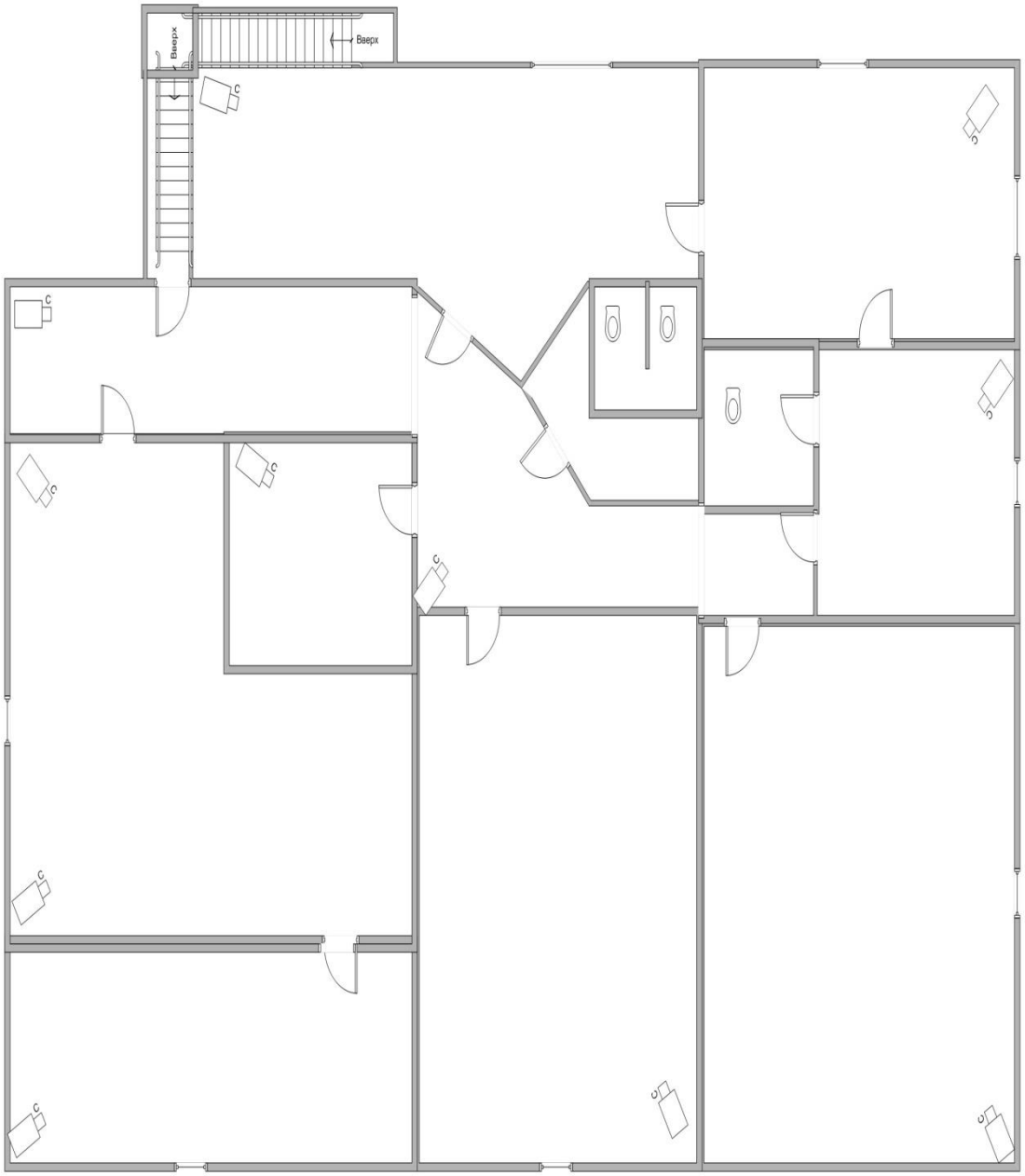


Рисунок В2 – Расположение элементов системы видеоконтроля второго этажа

Приложение Г

Схема расположений датчиков контроля доступа представлена на рисунке Г1 и Г2.

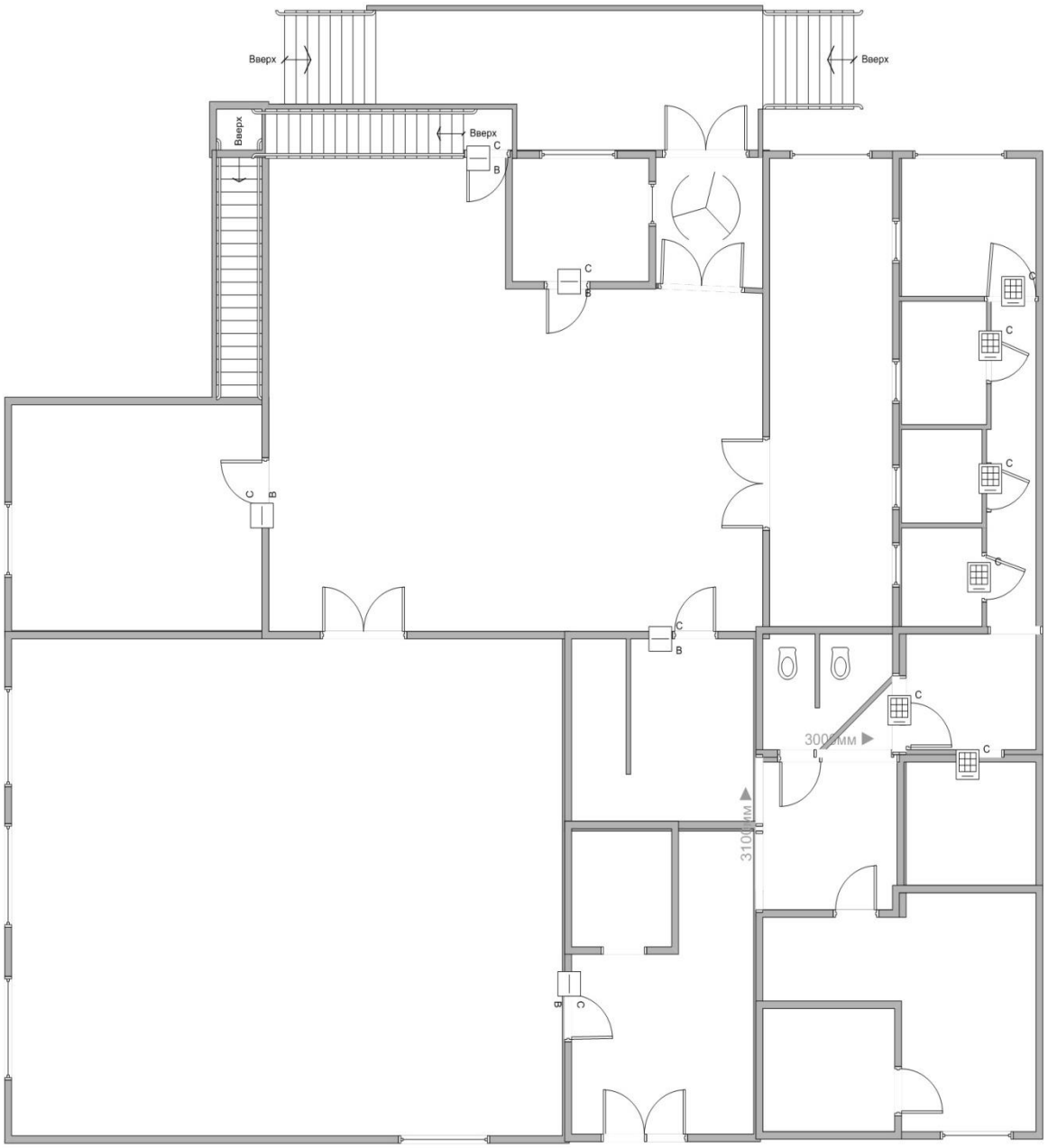


Рисунок Г1 – СКУД первый этаж

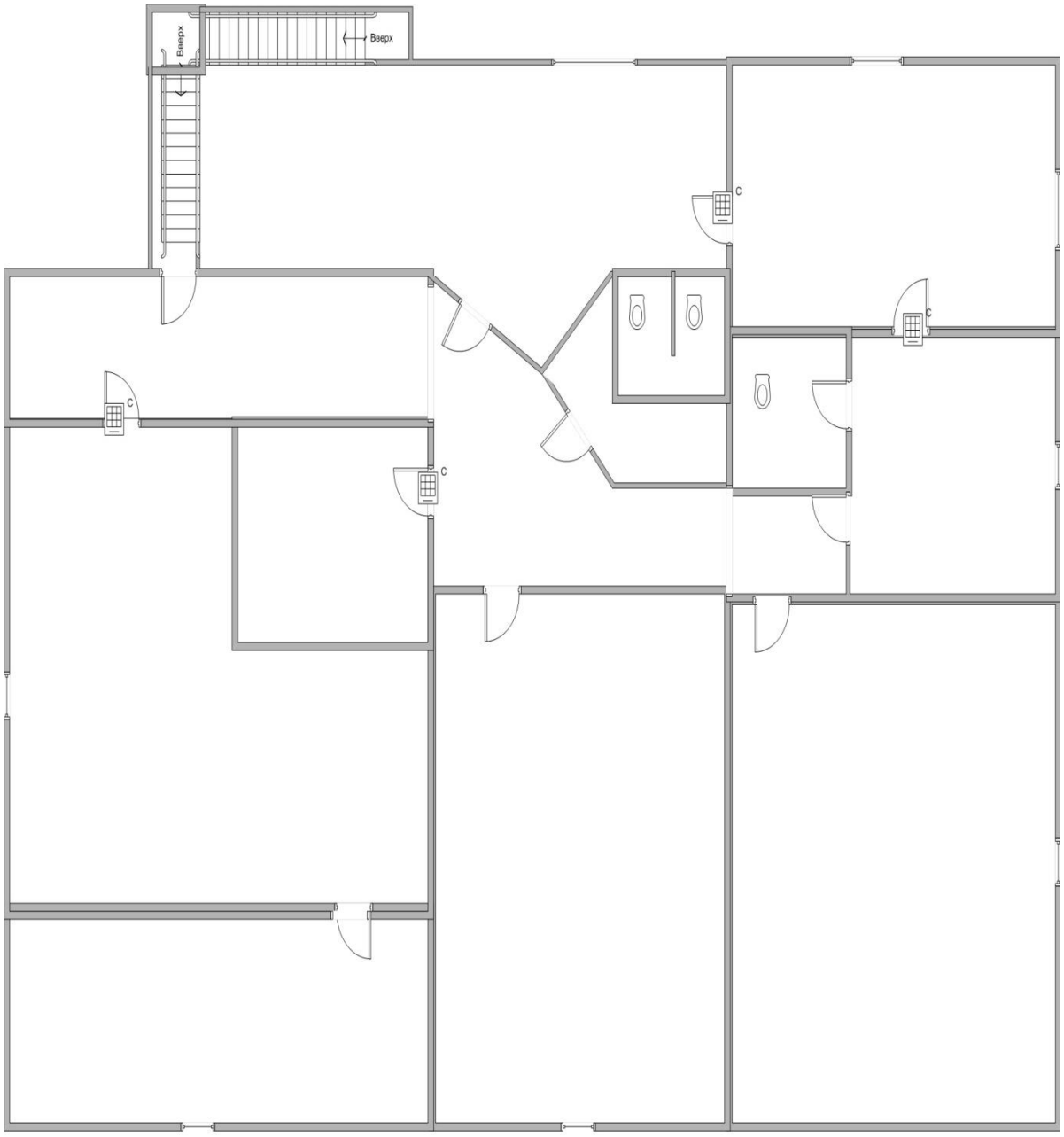


Рисунок Г2 – СКУД второй этаж

Приложение Д

Рабочая топология сети головного офиса и филиала представлена на рисунке Д1.

Доступ происходит из любого узла в любой узел. Это гарантирует связь двух офисов без перерывов.

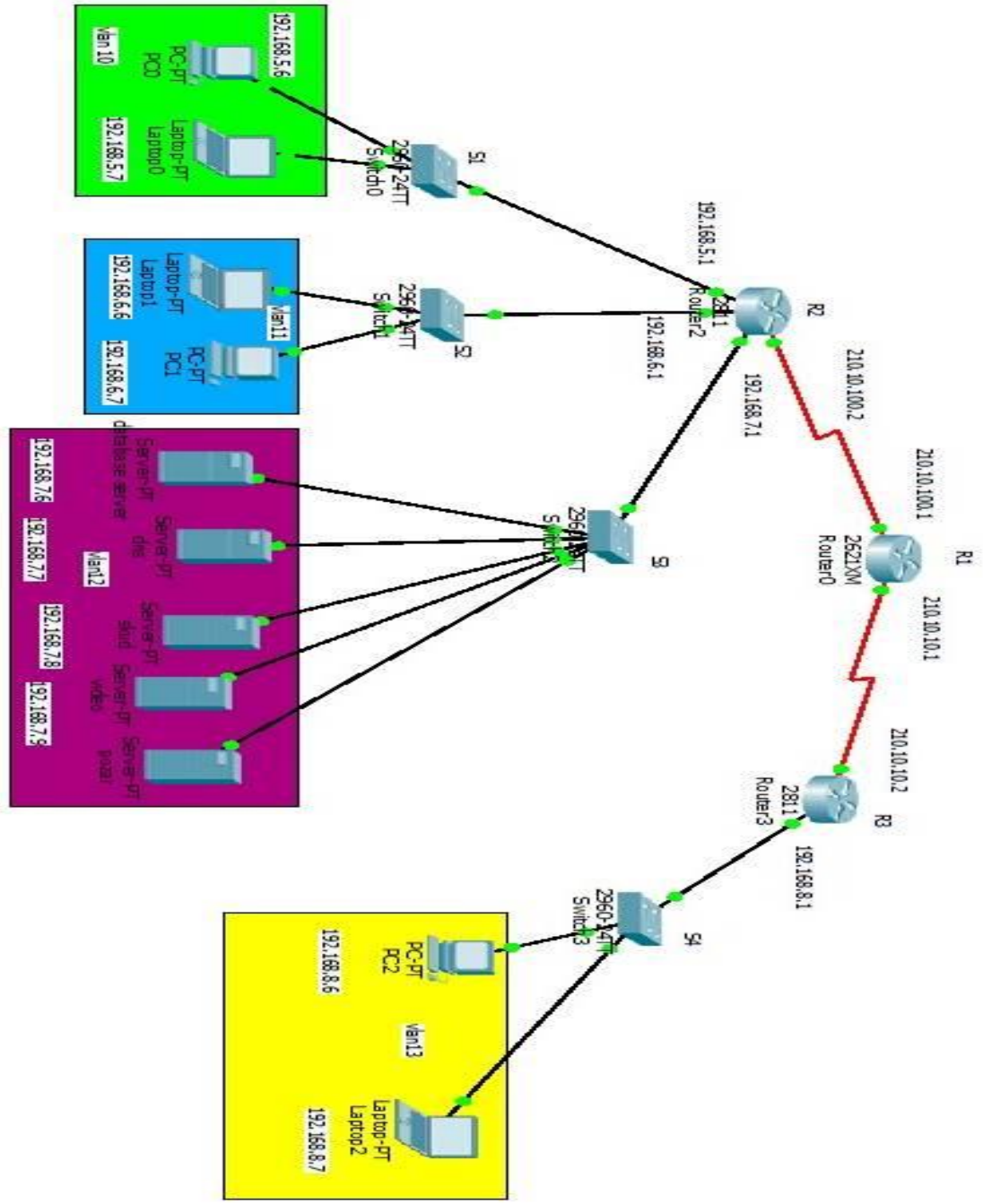


Рисунок Д1 – Топология сети

Приложение Е

Список основных команд интерфейса IOS CLI представлена в таблице Е1.

Т а б л и ц а Е 1 – Основные команды IOS

Команда	Описание
?	Выводит список доступных команд. После вывода одного экрана появляется приглашение —more—, указывающее, что на экран выведена не вся информация. Для построчного просмотра необходимо нажать *ENTER* или клавишу *ПРОБЕЛ*, для вывода следующего экрана.
enable	Переход в привилегированный режим. После ввода команды необходимо ввести пароль.
disable	Возврат в пользовательский режим.
exit, quit	Выход из любого режима и завершение сеанса работы с точкой доступа.
show	Вывести текущую информацию о системе.
configure terminal	Вход в режим конфигурации.
copy running–config startup–config	Скопировать текущую конфигурацию на место начальной.
shutdown	Отключение интерфейса.
no	Для отключения функционирования или полного изменения действия команды.
hostname *name*	Задание имени точки доступа.
dot11 mbssid	Включение на точке доступа возможности множественного идентификатора SSID. Используется для передачи в широковещательном пакете (beacon) более одного идентификатора сети (например, если существуют несколько виртуальных сетей).
dot11 ssid *ssid*	Глобальная настройка идентификатора SSID. Параметр *ssid* – название беспроводной сети.
dot11 vlan–name *name* vlan *ID*	Назначение имени для определенной виртуальной сети
power	Установка уровня мощности сигнала на точке доступа или клиенте.
speed	Установка скорости передачи данных.
encapsulation dot1q *ID* [native]	Активация виртуальной сети для радио интерфейса. Опция native назначает данную виртуальную сеть главной.
vlan *ID*	Определение идентификатора сети SSID к виртуальной сети. Для каждой виртуальной сети может быть создан только один SSID. Точки доступа поддерживают до 16 SSID.

Приложение Ж

Программа контроля доступа представлена на рисунке Ж1 представлена на рисунке Ж1 и Ж2.

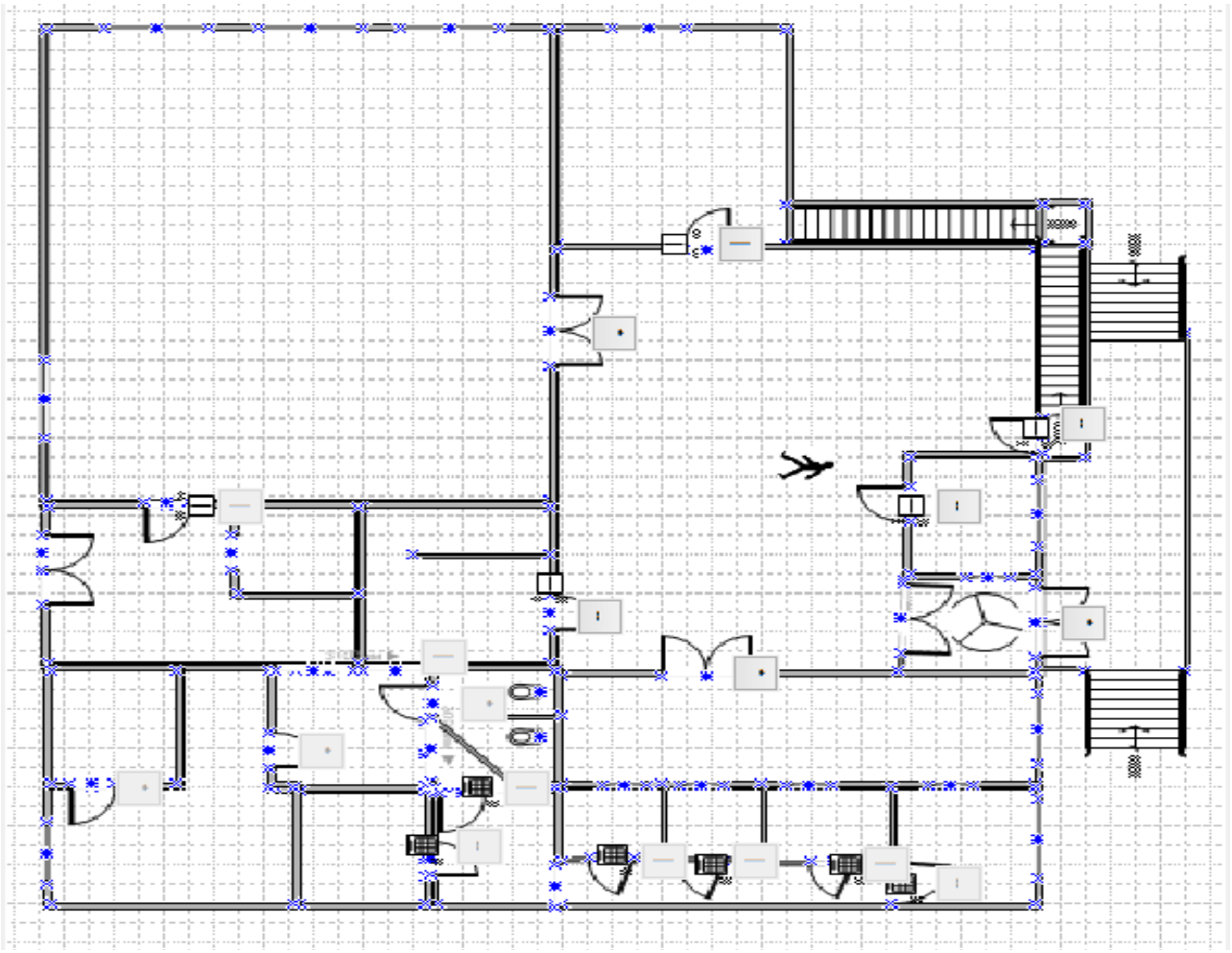


Рисунок Ж1 – Программа для реализации визуального представления контроля доступа

Окончание приложения Ж

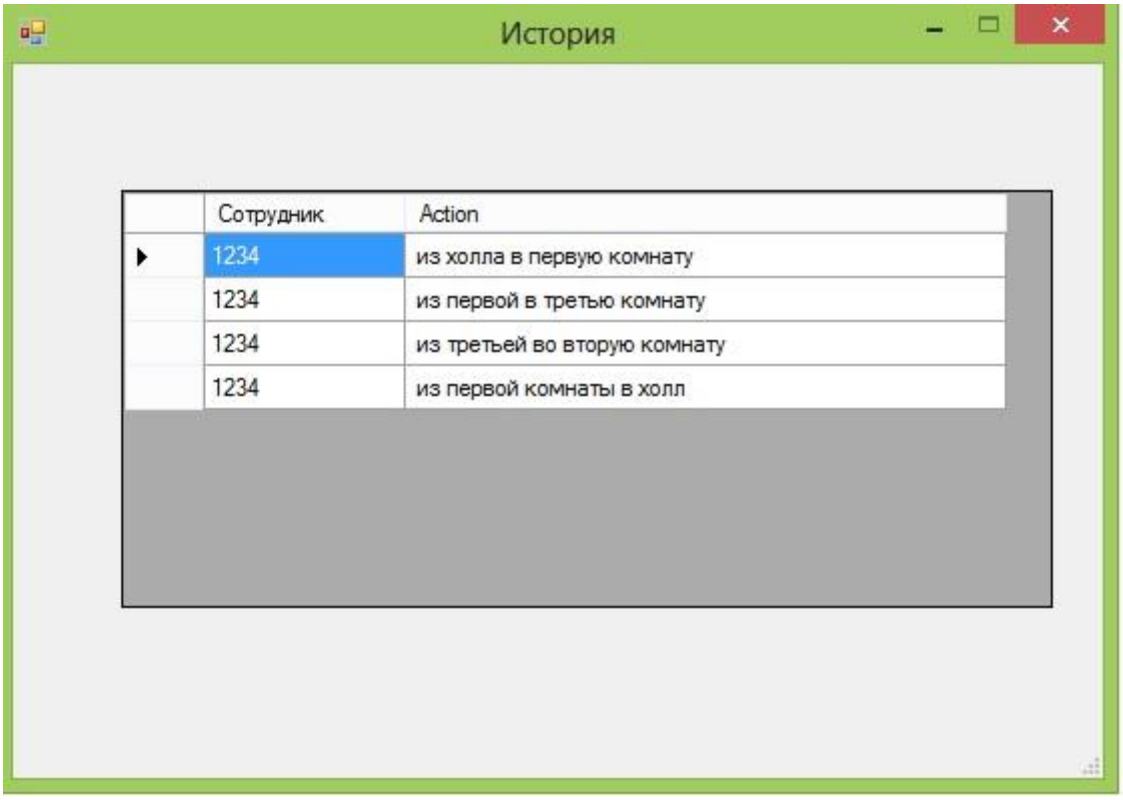


Рисунок Ж2 – Запись проходов через шлюз контроля доступа

Приложение 3

Настройка и конфигурация сетевого оборудования коммутаторов, маршрутов, камер, шлюзов контроля доступа, пожарных из вещателей и протоколов передачи данных:

Маршрутизатор R1

```
Router>enable
Router(config)#conf t
Router(config)#host name R1
R1(config)#int s 1/0
R1(config-if)#ip add  210.10.100.1 255.255.255.0
R1(config-if)# no sh
R1(config)#int s 0/0
R1(config-if)#ip add  210.10.10.1 255.255.255.0
R1(config-if)# no sh
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config)#password cisco
R1(config)#login
R1(config)#exit
R1(config)#router rip
R1(config-router)#network  210.10.100.0
R1(config-router)#network  210.10.10.0
R1(config-router)#exit
```

Маршрутизатор R2

```
Router>enable
Router(config)#conf t
Router(config)#host name R2
R2(config)#int s 0/1/0
R2(config-if)#ip add 210.10.100.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config-)# fa 0/1
R2(config-if)#ip add 192.168.5.1 255.255.255.0
R2(config-if)# no sh
R2(config-if)#exit
R2(config)#fa 0/0
R2(config-if)# ip add 192.168.6.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#Eth 0/1
R2(config-if)#ip add 192.168.7.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config-if)# ip route 210.10.10.0 255.255.255.0 210.10.100.1
R2(config-if)#exit
```

Маршрутизатор R3

```
Router>enable
Router(config)#conf t
Router(config)#host name R3
R3(config)#int s 1/1/0
R3(config-if)#ip add 210.10.10.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config-if)#int fa 0/0
R3(config-if)#ip add 192.168.8.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config-if)# ip route 210.10.100.0 255.255.255.0 210.10.10.1
R3(config-if)#exit
```

Коммутатор S1

```
Switch0>enable
Switch0>conf t
Switch0(config)>host name S1
S1(config)#enable password cisco
S1(config)#enable secret class
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1(config)#vlan 10
S1(config)#name vlan 10
S1(config)#interface fastethernet 0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#no shutdown
S1(config)#interface fastethernet 0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)# switchport mode trunk allowed vlan all
S1(config-if)#end
```

Коммутатор S2

```
Switch0>enable
Switch0>conf t
```

```
Switch0(config)>host name S2
S2(config)#enable password cisco
S2(config)#enable secret class
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#end
S2(config)#vlan 11
S2(config)#name vlan 11
S2(config)#interface fastethernet 0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 11
S2(config-if)#no shutdown
S2(config)#interface fastethernet 0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 11
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#interface fastethernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)# switchport mode trunk allowed vlan all
S2(config-if)#end
```

Коммутатор S3

```
Switch0>enable
Switch0>conf t
Switch0(config)>host name S3
S2(config)#enable password cisco
S2(config)#enable secret class
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#end
S2(config)#vlan 12
S2(config)#name vlan 12
S2(config)#interface fastethernet 0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
S2(config-if)#no shutdown
S2(config)#interface fastethernet 0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
S2(config-if)#no shutdown
S2(config)#interface fastethernet 0/4
```

```
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
S2(config-if)#no shutdown
S2(config)#interface fastethernet 0/5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
S2(config-if)#no shutdown
S2(config)#interface fastethernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#interface fastethernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)# switchport mode trunk allowed vlan all
S2(config-if)#end
```

Шлюз контроля доступа w1

```
Access>enable
Access>conf t
Access#host name W1
W1# ip add 192.168.12.2 255.255.255.0
W1#exit
```

Шлюз контроля доступа w2

```
Was>enable
Was>conf t
Was#host name W2
W1# ip add 192.168.12.8 255.255.255.0
W1#exit
```

Пожарная сигнализация Sc1

```
Pas>enable
Pas>conf t
Pas#host name sc1
sc# ip add 192.168.10.2 255.255.255.0
sc#exit
```

Пожарная сигнализация Sc2

```
Cas>enable
Cas>conf t
Cas#host name sc2
Sc2# ip add 192.168.10.42 255.255.255.0
Sc2#exit
```

Пожарная сигнализация Sc3

Kom>enable
Kom>conf t
Kom#host name sc3
Sc3# ip add 192.168.10.60 255.255.255.0
Sc3#exit

Видеоконтроль Kam1

Camera>enable
Camera >conf t
Camera #host name Kam1
Kam1# ip add 192.168.11.2 255.255.255.0
Kam1#exit

Видеоконтроль Kam2

Camera>enable
Camera >conf t
Camera #host name Kam2
Kam1# ip add 192.168.11.8 255.255.255.0
Kam1#exit