**ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КАЛУЖСКОЙ ОБЛАСТИ**

**«КАЛУЖСКИЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»**

**(ГАПОУ КО «КТК»)**

|  |  |
| --- | --- |
| Дипломная работа выполнена  и защищена с оценкой \_\_\_\_\_\_  Председатель ГЭК \_\_\_\_\_\_\_\_\_  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г | Допущена к защите  зам. директора по УТР  \_\_\_\_\_\_\_\_\_ / Л.Х. Метаки  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА   
(ДИПЛОМНАЯ РАБОТА)**

На тему: «Проектирование и реализация комплексной системы защиты информации на примере строительной компании»

**Студента:** Никулина Даниила Дмитриевича

(фамилия, имя, отчество)

**Специальность:** 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

**Квалификация:** Техник по защите информации

**Группа:** 4 ОИБ

**Руководитель дипломной работы \_\_\_\_\_\_\_\_\_\_\_ /** В.В. Голиков

**Консультанты: \_\_\_\_\_\_\_\_\_\_\_ /** О.А. Симонова

**г. Калуга, 2024**

**СОДЕРЖАНИЕ**

[Глава 1. Анализ теоретических основ организации 6](#_Toc169655780)

[1.1. Анализ исследуемой строительной компании 6](#_Toc169655781)

[1.2. Организационная структура строительной компании 9](#_Toc169655782)

[1.3. Объекты зашиты и угрозы информационной безопасности 13](#_Toc169655783)

[1.4. Анализ рисков и угроз для строительной компании 16](#_Toc169655784)

[1.5. Матрица безопасности строительной компании 20](#_Toc169655785)

[Глава 2. Реализация комплексной системы защиты 23](#_Toc169655786)

[2.1. Организация физической защиты 23](#_Toc169655787)

[2.1.1. Выбор запирающих средств и систем 25](#_Toc169655788)

[2.1.2. Выбор средств видеонаблюдения 33](#_Toc169655789)

[2.1.3. Выбор средств пожарно-охранной сигнализации 44](#_Toc169655790)

[2.2. Организация информационной защиты 52](#_Toc169655791)

[2.2.1. Описание информационной среды строительной компании 53](#_Toc169655792)

[2.2.2. Средства ограничения программной среды в системе защиты информации 56](#_Toc169655793)

[ГЛАВА 3. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАБОТ 68](#_Toc169655794)

[3.1. Расчет затрат на оборудование 68](#_Toc169655795)

[3.2. Расчет затрат на программное обеспечение 71](#_Toc169655797)

[3.3. Оценка экономической эффективности работы 71](#_Toc169655798)

[ЗАКЛЮЧЕНИЕ 73](#_Toc169655799)

[БИБЛИОГРАФИЯ 75](#_Toc169655800)

###### ВВЕДЕНИЕ

Обеспечение информационной безопасности в современных условиях приобретает особую значимость, поскольку информационные ресурсы стали одним из ключевых факторов успешной деятельности любой компании. Строительные компании, такие как "Калуга-Стройдом", сталкиваются с многочисленными угрозами информационной безопасности, которые могут привести к серьезным последствиям, включая утрату данных, финансовые потери и ущерб репутации.

Актуальность темы определяется необходимостью создания надежной системы защиты информации в условиях возрастающей сложности и числа киберугроз. Для строительной компании критически важно обеспечить безопасность как коммерческой, так и технической информации, включая проекты, сметы и данные сотрудников.

Новизна темы заключается в применении передовых методов и технологий для разработки комплексной системы защиты информации, адаптированной к специфике строительной отрасли.

Проблемой исследования является несоответствие между растущей потребностью в защите информации в строительной отрасли и отсутствием эффективных механизмов ее обеспечения.

Цель данной выпускной квалификационной работы заключается в проектировании и реализации комплексной системы защиты информации для строительной компании "Калуга-Стройдом".

Для достижения поставленной цели необходимо решить следующие задачи:

* провести анализ текущего состояния информационной безопасности в компании "Калуга-Стройдом";
* изучить существующие системы защиты информации;
* определить основные угрозы и риски информационной безопасности для строительной компании;
* разработать матрицу безопасности, включающую методы и средства защиты информации;
* выбрать оптимальные аппаратные и программные средства для реализации предложенной системы защиты.

Объектом исследования является информационная безопасность в деятельности строительной компании "Калуга-Стройдом". Это включает в себя анализ всех аспектов, связанных с защитой конфиденциальной информации, технических решений, процессов обработки данных, организационных мер и политик безопасности, а также управления доступом к информации.

Предметом исследования являются конкретные аспекты информационной безопасности в деятельности строительной компании "Калуга-Стройдом". Это включает в себя следующие аспекты:

* технологические решения и средства защиты;
* организационные меры безопасности;
* управление рисками;
* защита персональных данных;
* тестирование на проникновение и аудит безопасности.

Предмет исследования направлен на практическое применение результатов и отражается через предложение конкретных рекомендаций и мер по улучшению системы информационной безопасности компании "Калуга-Стройдом".

Результаты исследования по информационной безопасности компании "Калуга-Стройдом" представляют как теоретическую, так и практическую значимость. С теоретической точки зрения, они способствуют расширению научных знаний в области информационной безопасности, применяемой в строительной индустрии, а также формированию новых методологий и подходов к обеспечению информационной безопасности на предприятиях этого сектора.

С практической точки зрения, осуществление предложенных в исследовании мер по обеспечению информационной безопасности позволит компании "Калуга-Стройдом" эффективно защищать конфиденциальную информацию и предотвращать утечки данных.

Методы исследования включают в себя разнообразные подходы, в том числе теоретические и эмпирические методы. В ходе написания дипломной работы по информационной безопасности в компании "Калуга-Стройдом" были использованы следующие методы исследования:

* теоретический анализ литературы;
* эмпирический анализ;
* сравнительный анализ;
* опрос сотрудников;
* экспериментальные исследования.

Этот комплекс методов обеспечил качественное исследование информационной безопасности в компании "Калуга-Стройдом" и формирование практически значимых выводов и рекомендаций.

Базой исследования для данной дипломной работы выступает строительная компания "Калуга-Стройдом". Именно в рамках этой компании было проведено исследование информационной безопасности.

Структура дипломной работы включает в себя введение, главу 1 (аналитическая часть), главу 2 (практическая часть), глава 3 (экономическая часть), заключение, библиография, приложения.

# **Глава 1. Анализ теоретических основ организации**

# Анализ исследуемой строительной компании

В рамках данного раздела будет проведен анализ деятельности строительной компании "Калуга-Стройдом". Основное внимание будет уделено истории развития компании, а также основным методам и подходам, используемым в ее работе. Целью данного анализа является получение глубокого понимания текущего состояния и особенностей функционирования "Калуга-Стройдом", что позволит выявить ключевые аспекты ее работы и потенциальные направления для оптимизации и улучшения эффективности деятельности.

История развития строительной компании "Калуга-Стройдом" связана с уникальными этапами, определившими её структуру и позиционирование на рынке. Зарождение компании относится к 15-летнему периоду, в течение которого она стала лидером в сфере строительства домов, коттеджей и инфраструктурных объектов в регионе Калуга и Калужской области.

Начало деятельности компании связано с основанием и первыми строительными проектами, которые определили её специализацию в строительстве жилых и коммерческих объектов.

В течение следующих лет "Калуга-Стройдом" активно расширял свою деятельность, участвуя в различных частных и государственных проектах. Компания накопила богатый опыт и разработала более 100 типовых проектов малоэтажных домов и коттеджей.

На сегодняшний день "Калуга-Стройдом" остается одним из лидеров рынка строительства в регионе. Она продолжает реализацию крупных проектов и активно развивается, сфокусировавшись на высоком качестве строительства и инновационных подходах.

Сравнительный анализ с зарубежными аналогами позволил выделить ключевые особенности успешных строительных компаний за рубежом. Их опыт и практики в области управления проектами, применения новых технологий и подходов к дизайну могут служить ценным источником вдохновения и обучения для "Калуга-Стройдом". Результатом анализа стало выявление преимуществ и недостатков иностранных методик и их применимости в российских условиях.

Исторический анализ развития компании "Калуга-Стройдом" и сопоставление её с зарубежными аналогами позволяет понять ключевые факторы успеха и определить потенциал для дальнейшего роста и развития. Этот анализ является основой для формулирования стратегических целей и рекомендаций компании в условиях современного рынка строительных услуг.

В дополнение к анализу деятельности "Калуга-Стройдом" будет осуществлен сравнительный анализ существующих подходов и методов в области строительства. Данный анализ позволит выявить наиболее эффективные и оптимальные методы решения проблем, с которыми сталкивается компания.

На основе проведенного сравнительного анализа будет обоснован выбор наиболее подходящего метода решения для решения исследуемой проблемы. Возможно, будет предложен собственный метод, адаптированный к особенностям компании "Калуга-Стройдом" и современным требованиям рынка строительства.

Этот раздел будет представлен подробным изложением выбранного метода решения, включая его принципы, этапы реализации и ожидаемые результаты. Подробное изложение позволит читателям понять, как выбранный метод сможет быть успешно внедрен в практику компании и каким образом он будет способствовать улучшению ее деятельности.

В рамках первого раздела также будет проведен анализ современного состояния проблемы, связанной с деятельностью строительной компании "Калуга-Стройдом", а также выявление тенденций развития данного процесса. Для этого будут использованы различные источники информации, включая действующие нормативные документы, данные официальной статистики, а также материалы аналитических обзоров и научных журнальных статей.

Анализ нормативных документов позволит оценить влияние законодательства на деятельность строительной отрасли в целом и на компанию "Калуга-Стройдом" в частности. Данные официальной статистики позволят выявить текущие тенденции и динамику развития строительного рынка, а также установить ключевые проблемные моменты, с которыми сталкиваются строительные компании в современных условиях.

Материалы аналитических обзоров и научных журнальных статей предоставят дополнительную экспертную информацию о текущем состоянии и перспективах развития строительной отрасли. Эти источники позволят глубже понять основные вызовы и возможности, с которыми сталкивается компания "Калуга-Стройдом", а также определить наиболее эффективные стратегии развития в будущем.

В рамках анализа современного состояния проблемы, связанной с деятельностью строительной компании "Калуга-Стройдом", будут рассмотрены следующие конкретные примеры:

* нормативные документы: изучение действующих нормативных актов в области строительства, таких как Градостроительный кодекс Российской Федерации, Закон о строительстве, а также местные нормативные акты Калужской области и города Калуги. Примером может служить анализ требований к проектированию и строительству объектов различного типа, а также нормативов в области безопасности труда и экологии;
* данные официальной статистики: изучение статистических данных о объеме строительной деятельности в Калужской области и городе Калуге за последние несколько лет. Примером может быть анализ динамики строительства жилых и коммерческих объектов, а также изменений в объеме инвестиций в строительство;
* материалы аналитических обзоров и научных журнальных статей: изучение результатов аналитических обзоров рынка недвижимости и строительства, проводимых агентствами и исследовательскими организациями. Примером может служить анализ статей о текущих тенденциях в развитии строительной отрасли, новых технологиях и методах управления проектами.

Конкретные примеры и данные из указанных источников позволят получить объективное представление о текущем состоянии и перспективах развития строительной отрасли в регионе, что будет являться основой для дальнейшего анализа и разработки рекомендаций в рамках дипломной работы.

В заключении данного раздела можно подчеркнуть значимость проведенного анализа исследуемой строительной компании "Калуга-Стройдом". Анализ позволил глубже понять особенности ее деятельности, выявить сильные стороны и проблемные моменты, а также определить потенциальные направления для улучшения деятельности и повышения конкурентоспособности на рынке.

Благодаря изучению нормативных актов, статистических данных и научных исследований удалось выявить основные факторы, влияющие на деятельность строительной отрасли в регионе. Также проведенный сравнительный анализ различных методов решения проблемы позволил определить наиболее эффективные подходы и методы управления проектами в сфере строительства.

Заключительные выводы и рекомендации, сформулированные на основе проведенного анализа, будут служить основой для дальнейшего изучения и разработки стратегии развития компании "Калуга-Стройдом". Это позволит компании успешно адаптироваться к изменяющимся условиям рынка и достичь новых высот в своей деятельности.

# Организационная структура строительной компании

Организационная структура строительной компании "Калуга-Стройдом" представляет собой слаженную систему подразделений и функций, направленных на эффективное выполнение строительных проектов. На вершине этой структуры находится генеральный директор, который определяет стратегические цели компании и координирует ее деятельность (рисунок 1).

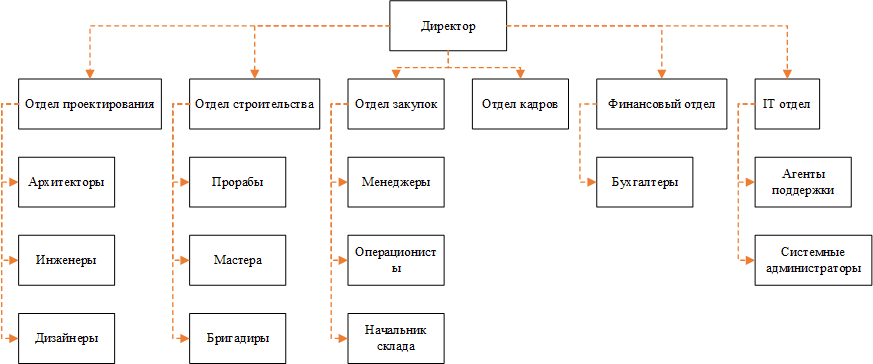


Рисунок 1 – Структура строительной компании

Под руководством генерального директора функционируют ключевые подразделения компании.

Отдел проектирования в компании "Калуга-Стройдом" играет ключевую роль в подготовке проектов строительства, начиная от первоначальной концепции и заканчивая детальными техническими спецификациями.

Архитекторы отдела проектирования отвечают за разработку концептуальных и архитектурных решений. Они проводят анализ местности, рельефа и климатических особенностей для оптимального планирования объектов.

Инженеры в отделе проектирования занимаются разработкой инженерных систем и коммуникаций. Они проектируют системы отопления, вентиляции, кондиционирования, электроснабжения, водоснабжения и канализации, учитывая особенности конкретного объекта и требования к его функциональности и энергоэффективности.

Дизайнеры в отделе проектирования ответственны за создание эстетического облика здания и его интерьеров. Они разрабатывают дизайн-проекты, подбирают отделочные материалы, мебель и декоративные элементы, чтобы создать гармоничное и стильное пространство.

Отдел строительства в структуре компании "Калуга-Стройдом" играет важную роль в обеспечении качественного и своевременного выполнения строительных проектов. Этот подразделение ответственно за координацию всех этапов строительства, начиная от подготовки площадки и заканчивая сдачей объекта заказчику.

Ключевые функции отдела строительства включают в себя организацию рабочих бригад, контроль выполнения строительных работ в соответствии с проектом и строительными стандартами, а также обеспечение безопасности на строительной площадке.

Таким образом, отдел строительства в компании "Калуга-Стройдом" является ключевым звеном в процессе реализации строительных проектов, обеспечивая их успешное выполнение в соответствии с высокими стандартами качества и безопасности.

Отдел по закупкам и снабжению в компании "Калуга-Стройдом" играет важную роль в обеспечении строительных проектов всем необходимым оборудованием, материалами и инструментами. Этот отдел ответственен за поиск и выбор надежных поставщиков, заключение договоров на выгодных условиях, а также за контроль качества и своевременность поставок.

Главная задача отдела закупок - обеспечить строительные объекты всем необходимым в нужном объеме и вовремя.

Кроме того, отдел закупок ведет контроль за качеством поставляемых материалов и оборудования, чтобы гарантировать их соответствие стандартам и требованиям заказчика. Он также отвечает за оптимизацию процесса закупок, минимизацию издержек и обеспечение эффективного использования ресурсов компании.

Отдел кадров и административного управления в компании "Калуга-Стройдом" играет важную роль в формировании и управлении человеческими ресурсами, а также в обеспечении эффективного функционирования внутренних процессов.

Одной из ключевых задач отдела кадров является найм и подбор квалифицированных специалистов для различных подразделений компании. Отдел кадров активно взаимодействует с руководителями отделов и менеджерами проектов для определения потребностей в персонале и поиска наиболее подходящих кандидатов на вакансии.

Помимо этого, отдел кадров и административного управления отвечает за ведение учета трудовых ресурсов, решение административных вопросов и поддержание порядка в офисе. Он обеспечивает выполнение трудового законодательства, регулирует отпуска и больничные листы, а также занимается организацией мероприятий для сотрудников компании.

Финансовый отдел и бухгалтерия в компании "Калуга-Стройдом" играют ключевую роль в эффективном управлении финансовыми ресурсами и обеспечении прозрачности бухгалтерского учета.

Бухгалтерия занимается ведением бухгалтерских документов, составлением финансовых отчетов и соблюдением всех законодательных и налоговых требований. Она отвечает за корректное оформление бухгалтерской отчетности, включая составление балансов, отчетов о прибылях и убытках, а также налоговых деклараций.

В заключении можно подчеркнуть ключевую роль каждого подразделения в общей деятельности компании и их важность для успешной реализации строительных проектов. Организационная структура компании обеспечивает эффективное управление ресурсами, оптимизацию производственных процессов и качественное выполнение заказов.

IT отдел выполняет несколько ключевых функций. Во-первых, управление инфраструктурой: планирование, развертывание и обслуживание IT инфраструктуры компании, включая серверы, рабочие станции, сетевые устройства и системы хранения данных. Во-вторых, поддержка программного обеспечения: обеспечение функционирования всех используемых программных продуктов, включая операционные системы, СУБД и специализированное ПО для проектирования и управления строительными проектами. В-третьих, безопасность информации: реализация мер по защите данных, включая установку антивирусного ПО, межсетевых экранов, систем обнаружения вторжений и регулярное обновление ПО. В-четвертых, управление пользователями и доступом: создание и управление учетными записями, настройка прав доступа к различным системам и данным. В-пятых, поддержка и обслуживание: своевременное обновление и ремонт оборудования и программного обеспечения для минимизации времени простоя и поддержания высокой производительности.

Техническая поддержка является неотъемлемой частью IT инфраструктуры строительной компании. Ее основная задача – оперативное решение возникающих у сотрудников проблем, связанных с IT оборудованием и программным обеспечением, а также клиентов компании.

Таким образом, организационная структура компании "Калуга-Стройдом" является основой для успешного функционирования и развития. Эффективное взаимодействие всех подразделений позволяет компании достигать высоких результатов в своей деятельности, обеспечивая клиентам качественные строительные услуги и удовлетворяя их потребности.

# Объекты зашиты и угрозы информационной безопасности

В современном информационном обществе, где данные играют ключевую роль в деятельности компаний, обеспечение их защиты становится приоритетной задачей для всех организаций. В данном контексте особое значение приобретает анализ объектов защиты и угроз информационной безопасности, осуществляемый в рамках дипломного исследования.

Информационная безопасность становится одним из важнейших аспектов деятельности строительных компаний, которые, как и многие другие субъекты бизнеса, активно используют цифровые технологии и хранят значительные объемы конфиденциальных данных. В связи с этим введение в анализ объектов защиты и угроз информационной безопасности строительной компании должно охватить широкий спектр вопросов, связанных с сохранностью данных, конфиденциальностью информации и обеспечением функционирования информационных систем без сбоев.

Прежде всего, необходимо провести анализ самых ценных активов компании, которые подвергаются рискам в области информационной безопасности. В эту категорию могут входить персональные данные клиентов, корпоративные секреты, интеллектуальная собственность, финансовые ресурсы и инфраструктура информационных систем.

Для полноценного анализа угроз и возможностей защиты информации необходимо учитывать как внутренние, так и внешние факторы, включая возможные технические неисправности, человеческие ошибки, а также целенаправленные кибератаки и другие формы внешних угроз. Кроме того, важно учитывать актуальные тренды в области информационной безопасности, включая последние разработки в сфере технологий защиты и методов атак.

Таким образом, введение в анализ объектов защиты и угроз информационной безопасности строительной компании должно дать обзор основных аспектов, которые будут рассмотрены далее в рамках данного раздела дипломной работы.

Конкретные объекты защиты информации в строительной компании включают:

* персональные данные клиентов и сотрудников. Это включает в себя их имена, адреса, контактные данные, информацию о доходах и другие личные сведения. Несанкционированный доступ к такой информации может привести к утечке конфиденциальных данных, нарушению приватности и даже краже личной идентичности;
* корпоративные секреты и интеллектуальная собственность. Это может включать в себя конфиденциальные планы проектов, технические спецификации, патенты, а также коммерческие сведения о клиентах и партнерах. Утечка такой информации может нанести серьезный ущерб репутации компании и привести к конкурентным преимуществам для конкурентов;
* финансовые данные. Сюда входят бухгалтерская отчетность, информация о доходах и расходах, банковские реквизиты и договоры с клиентами. Несанкционированный доступ к этим данным может привести к финансовым потерям, мошенничеству и нарушению законодательства о защите данных;
* информационная инфраструктура. Это включает в себя серверы, базы данных, сетевое оборудование и программное обеспечение, используемое для хранения, обработки и передачи информации. Компрометация информационной инфраструктуры может привести к отказу систем, утечке данных и потере доступа к критическим ресурсам;
* критическая инфраструктура. Некоторые строительные компании могут управлять критической инфраструктурой, такой как энергетические системы, водоснабжение и транспортные сети. Несанкционированный доступ к таким системам может иметь серьезные последствия для безопасности и комфорта населения.

Конкретные примеры угроз информационной безопасности для строительной компании включают:

* кибератаки. Нападения хакеров на информационные системы компании с целью получения несанкционированного доступа к конфиденциальным данным, внедрения вредоносного программного обеспечения или блокировки работы сети;
* фишинг. Атаки, при которых злоумышленники маскируются под доверенные источники, например, отправляя фальшивые электронные письма от банков, государственных органов или других компаний с целью получения личной информации или учетных данных сотрудников;
* утеря или кража устройств. Потеря или кража ноутбуков, планшетов или мобильных телефонов с корпоративной информацией на них может привести к утечке конфиденциальных данных;
* социальная инженерия. Злоумышленники могут пытаться манипулировать сотрудниками компании, например, звоня по телефону и представляясь сотрудниками службы поддержки, чтобы получить доступ к конфиденциальным данным или учетным записям;
* неосторожное обращение с данными. Ошибка в настройках безопасности, неправильное хранение или передача конфиденциальной информации могут привести к утечке данных или доступу к ним несанкционированными лицами;
* физические угрозы. Кража или разрушение физического оборудования компании, такого как серверы или сетевое оборудование, может привести к потере данных или нарушению работы информационных систем.

В заключении к пункту можно подчеркнуть, что обеспечение информационной безопасности является важным аспектом деятельности строительных компаний в современном цифровом мире. В связи с этим, необходимо уделить особое внимание защите конфиденциальной информации, обеспечению непрерывности бизнес-процессов и предотвращению утечек данных.

Определены ключевые объекты защиты, включая информационные системы компании, базы данных клиентов, технологические процессы и персональные данные сотрудников. Проведен анализ угроз информационной безопасности, включая кибератаки, вредоносное программное обеспечение, фишинг, утерю устройств и физические вторжения.

Для эффективной защиты от угроз информационной безопасности рекомендуется принятие комплекса мер, включающих технические, организационные и обучающие аспекты. Компания должна инвестировать в современные системы защиты, регулярно обновлять программное обеспечение, обучать сотрудников правилам безопасности и осуществлять контроль за доступом к конфиденциальной информации.

В целом, эффективная защита информации является неотъемлемой частью успешного функционирования строительной компании, а управление рисками информационной безопасности должно быть приоритетным направлением ее деятельности.

# Анализ рисков и угроз для строительной компании

Пункт вводит в себя важный аспект исследования, направленный на оценку возможных опасностей и угроз, с которыми может столкнуться строительная компания в процессе своей деятельности. Осуществление такого анализа позволяет выявить потенциальные риски, которые могут негативно повлиять на выполнение проектов, финансовое состояние и репутацию компании.

Данный пункт включает обзор контекста, в котором функционирует строительная компания, и указание на важность анализа рисков в сфере строительства. Это также может включать обоснование необходимости управления рисками для обеспечения безопасности проектов, эффективного использования ресурсов и минимизации потерь.

В целях повышения полноты анализа рисков и угроз важно учитывать как внутренние факторы, такие как финансовое состояние компании, ее технические возможности и управленческий опыт, так и внешние факторы, такие как экономическая нестабильность, изменения в законодательстве и конкурентная среда.

Обобщая, введение пункта выступает в качестве отправной точки для более глубокого изучения и оценки потенциальных рисков, с которыми может столкнуться компания в своей деятельности, и позволяет обосновать необходимость проведения анализа рисков в рамках данного исследования.

В контексте строительной компании, анализ рисков является неотъемлемой частью процесса управления, поскольку строительство подвержено множеству потенциальных опасностей и угроз. Рассмотрим некоторые из них более подробно.

* Финансовые риски. Это могут быть колебания цен на строительные материалы, изменения валютных курсов, задержки в оплате заказчиками. Например, если компания заключает контракт на строительство объекта при нынешних ценах на строительные материалы, но к моменту начала работ эти цены возрастут, это может значительно увеличить затраты компании.
* Технические риски. Связаны с возможными техническими проблемами во время строительства или после его завершения. Например, неожиданные геологические особенности, несоответствие проекта реальным условиям строительства, а также технические неисправности после сдачи объекта.
* Юридические риски. Включают в себя возможные споры с заказчиками, нарушения законодательства, претензии со стороны третьих лиц и т.д. Например, неправильно составленный договор или неправомерные действия работников могут привести к дорогостоящим судебным разбирательствам.
* Риски в области безопасности и здоровья. Это опасности, связанные с травмами рабочих на стройплощадке, авариями и профессиональными заболеваниями. Например, падение с высоты, поражение электрическим током или вредные воздействия вредных веществ.
* Экологические риски. Связаны с негативными воздействиями на окружающую среду в процессе строительства. Например, загрязнение почвы, водоемов или атмосферы, нарушение экологических стандартов.
* Репутационные риски. Связаны с возможным повреждением репутации компании в результате отрицательных отзывов заказчиков, небрежности в работе или невыполнения обязательств. Например, задержки в сроках строительства или низкое качество выполняемых работ.

Каждый из этих рисков имеет потенциал нанести ущерб как финансовому состоянию компании, так и ее репутации. Поэтому для успешного управления рисками строительная компания должна систематически анализировать и оценивать их, разрабатывать стратегии смягчения последствий и внедрять соответствующие меры предосторожности.

Строительная компания подвержена различным угрозам, которые могут негативно сказаться на ее деятельности и результативности проектов. Рассмотрим некоторые из наиболее распространенных угроз:

* финансовые угрозы. Это могут быть неоплаченные счета, невыполнение заказчиком обязательств по оплате работ, увеличение стоимости строительных материалов и услуг. Например, отсутствие финансирования со стороны заказчика или задержки в выплате средств могут привести к финансовым трудностям для компании;
* технические угрозы. Возможны технические сбои оборудования, ошибки в проектировании, изменения в проекте во время строительства и другие технические проблемы. Например, неисправности кранов, отклонения от проекта или непредвиденные геологические условия могут замедлить выполнение работ и увеличить затраты;
* юридические угрозы. Компания может столкнуться с судебными исками, претензиями со стороны заказчиков, неправомерными действиями подрядчиков или нарушениями законодательства. Например, споры о качестве работ, нарушения трудового законодательства или правонарушения в области защиты окружающей среды;
* угрозы в области безопасности и здоровья. Это могут быть травмы и несчастные случаи на рабочих местах, несоблюдение правил безопасности, аварии на стройплощадке и другие опасности для работников. Например, падение с высоты, поражение электрическим током или инциденты с тяжелым оборудованием;
* экологические угрозы. Компания может столкнуться с претензиями о загрязнении окружающей среды, нарушениях экологических стандартов, уничтожении природных ресурсов и другими экологическими проблемами. Например, неправильная утилизация отходов, выбросы вредных веществ или загрязнение водоемов;
* информационные угрозы. Возможно нарушение конфиденциальности данных, кибератаки, утечки информации о проектах или другие информационные инциденты. Например, хакерские атаки на системы компании, утечка конфиденциальной информации или вирусные атаки на компьютерные сети.

Кроме вышеперечисленных, строительная компания также подвержена физическим угрозам, которые могут привести к существенным потерям и проблемам:

* взломы и кражи. Несанкционированный доступ на строительные площадки или в офисы компании может привести к краже материалов, инструментов, оборудования или документации. Например, кража строительных материалов со стройплощадки или взлом офиса для получения ценной информации о проектах и заказах;
* саботаж и марадерство. Происшествия, такие как поджоги, вандализм или разрушение оборудования, могут нанести серьезный ущерб компании и привести к задержкам в выполнении проектов. Например, саботажные действия против оборудования или инфраструктуры на стройплощадке, что может привести к остановке работ и финансовым потерям;
* природные катастрофы. Строительные объекты могут быть повреждены из-за стихийных бедствий, таких как наводнения, землетрясения, пожары или ураганы. Это может привести к разрушению материалов, оборудования, инфраструктуры и даже к потере человеческих жизней. Например, разрушение строений из-за землетрясения или повреждение оборудования от пожара;
* технические аварии и поломки. Неисправности и аварии на оборудовании, такие как аварии строительной техники, порча строительных материалов или инструментов, могут привести к остановке работ и дополнительным затратам на восстановление и замену оборудования. Например, поломка крана на стройплощадке или повреждение строительных материалов в результате неправильной эксплуатации.

Все эти угрозы требуют внимательного анализа и разработки соответствующих мер по защите и предотвращению возможных инцидентов.

Анализ рисков и угроз для строительной компании позволяет выявить потенциальные опасности и проблемы, с которыми она может столкнуться в своей деятельности. Исследование различных видов угроз, включая информационные, финансовые, операционные и физические, позволяет компании лучше понять свои уязвимые места и разработать стратегии по их предотвращению или смягчению последствий.

В результате анализа рисков и угроз строительная компания может принять необходимые меры по улучшению системы безопасности, обучению персонала, внедрению современных технологий и разработке планов действий в случае возникновения чрезвычайных ситуаций. Это позволит снизить вероятность возникновения проблем и минимизировать потенциальные убытки, обеспечивая более стабильную и безопасную работу компании.

В целом, анализ рисков и угроз для строительной компании является важным этапом ее деятельности, который помогает обеспечить надежную защиту интересов компании, ее сотрудников и заказчиков.

# Матрица безопасности строительной компании

Матрица безопасности является инструментом, который позволяет строительным компаниям систематизировать и анализировать потенциальные угрозы и риски, с которыми они могут столкнуться в процессе своей деятельности. В контексте строительной компании "Калуга-Стройдом" матрица безопасности представляет собой инструмент управления рисками, направленный на обеспечение безопасности работников, клиентов и ресурсов компании.

Основные элементы матрицы безопасности включают в себя:

* идентификация угроз и рисков. В первую очередь необходимо провести анализ и выявить потенциальные угрозы и риски, которые могут повлиять на деятельность строительной компании "Калуга-Стройдом". Это могут быть как внутренние факторы, такие как недостаточная квалификация персонала или несоответствие стандартам безопасности, так и внешние факторы, например, изменения законодательства или неблагоприятные погодные условия;
* оценка вероятности и воздействия. После идентификации угроз и рисков необходимо оценить их вероятность возникновения и потенциальное воздействие на деятельность компании. Некоторые угрозы могут иметь более высокую вероятность возникновения и более серьезное воздействие, чем другие, и должны быть рассмотрены с приоритетом;
* разработка стратегий управления рисками. На основе оценки угроз и рисков необходимо разработать стратегии по их управлению и минимизации. Это может включать в себя разработку процедур безопасности, обучение персонала, заключение страховых полисов, использование специализированного оборудования и т. д.

Примеры угроз и рисков для строительной компании "Калуга-Стройдом" включают в себя:

* травмы на рабочем месте. Возможные травмы, связанные с использованием строительного оборудования, падением с высоты, несоблюдением правил безопасности и т. д.;
* пожары и взрывы. Риск возгорания на строительной площадке из-за неправильного хранения или использования материалов, несоответствия электрооборудования стандартам безопасности и т. д.;
* кражи и вандализм. Угроза кражи строительного материала, инструментов или оборудования, а также вандализма на объектах строительства;
* несоблюдение правовых норм и стандартов. Риск возникновения судебных и финансовых проблем из-за нарушения законодательства в области безопасности и строительства.

На основе анализа угроз и рисков компания "Калуга-Стройдом" может разработать и реализовать соответствующие меры по управлению рисками, чтобы обеспечить безопасность своей деятельности, своих сотрудников и заказчиков.

В заключении к пункту следует отметить, что разработка и использование матрицы безопасности являются важным инструментом для эффективного управления рисками и обеспечения безопасности в деятельности строительной компании "Калуга-Стройдом".

Анализирование потенциальных угроз и рисков позволяет идентифицировать уязвимые места в деятельности компании и принимать соответствующие меры для их предотвращения или минимизации. Наличие четкой и структурированной матрицы безопасности позволяет руководству и персоналу компании осознанно подходить к вопросам безопасности и оперативно реагировать на угрозы.

Кроме того, матрица безопасности способствует повышению эффективности управления рисками, улучшению качества работы и снижению финансовых потерь, связанных с инцидентами и авариями. Регулярное обновление и адаптация матрицы в соответствии с изменяющимся бизнес-окружением и новыми угрозами позволяет строительной компании "Калуга-Стройдом" оставаться конкурентоспособной и успешной на рынке.

Таким образом, разработка и использование матрицы безопасности являются неотъемлемой частью стратегии безопасности и рискового менеджмента компании, что способствует ее устойчивому развитию и процветанию в условиях современной бизнес-среды.

# **Глава 2. Реализация комплексной системы защиты**

# 2.1. Организация физической защиты

Для строительной компании "Калуга-Стройдом" организация физической защиты является неотъемлемой частью общей системы безопасности. Она включает в себя несколько важных этапов, начиная с анализа уязвимостей и потребностей компании. Этот этап включает в себя детальное изучение объектов компании, их локаций и характеристик, а также оценку рисков для различных зон доступа, складов, офисов и строительных объектов.

На основе анализа уязвимостей и потребностей разрабатывается план физической защиты. В этом плане определяются мероприятия, необходимые для обеспечения безопасности компании, включая выбор и установку оборудования, организацию систем контроля доступа и видеонаблюдения, а также меры безопасности для защиты персонала (рисунок 2).



Рисунок 2 – Схема офиса строительной компании

После разработки плана физической защиты осуществляется установка необходимого оборудования. Это включает в себя установку замков, сейфов, систем видеонаблюдения, пожарных и охранных сигнализаций в соответствии с требованиями безопасности компании.

Однако не менее важным является обучение персонала компании. Сотрудники должны быть ознакомлены с процедурами безопасности, правилами доступа, использования оборудования и мерами реагирования на чрезвычайные ситуации.

После установки оборудования и обучения персонала система физической защиты регулярно обновляется и тестируется на работоспособность. Это включает в себя проверку оборудования, обучение персонала новым методам защиты и анализ последних тенденций в области безопасности.

Организация физической защиты играет ключевую роль в обеспечении безопасности информации на объекте. Важно обеспечить защиту как серверных помещений, где хранятся ценные данные и информационные ресурсы компании, так и обычных рабочих помещений, где работают сотрудники.

Для серверных помещений физическая защита включает в себя установку современных систем контроля доступа с использованием электронных замков, биометрических средств и систем видеонаблюдения для ограничения доступа только авторизованных сотрудников. Также важно размещение серверов в специально оборудованных помещениях с ограниченным доступом, обеспечивающих контроль температуры, влажности и других условий, необходимых для надежной работы оборудования. Использование систем детекции и пожаротушения также обязательно для своевременного обнаружения и ликвидации возможных угроз пожара или короткого замыкания.

Для обычных рабочих помещений физическая защита включает в себя установку средств видеонаблюдения в зонах общего доступа для контроля за передвижением персонала и предотвращения несанкционированного доступа. Также важно обеспечить доступ только авторизованным сотрудникам с помощью ключевых карт или кодовых замков, а также обеспечить безопасность технического оборудования от случайного повреждения или кражи.

Таким образом, организация физической защиты для строительной компании "Калуга-Стройдом" включает в себя анализ рисков, разработку и реализацию плана мероприятий, обучение персонала и постоянное обновление системы для обеспечения эффективной защиты объектов компании.

# 2.1.1. Выбор запирающих средств и систем

В условиях современного бизнеса, где безопасность является одним из приоритетных аспектов, выбор и установка запирающих средств и систем играют ключевую роль в обеспечении безопасности объектов компании. В данной главе будет рассмотрен вопрос выбора таких средств и систем для строительной компании "Калуга-Стройдом". Анализ и выбор оптимальных запирающих механизмов, замков, и систем контроля доступа являются необходимыми шагами для обеспечения надежной защиты как физических, так и информационных ресурсов компании.

Целью данного раздела является представление анализа существующих запирающих механизмов и систем контроля доступа, а также выбор наиболее подходящих вариантов для конкретных потребностей и особенностей деятельности строительной компании "Калуга-Стройдом".

Описание схемы здания с запирающими средствами и контролем доступа включает установку различных типов запирающих устройств и систем контроля доступа в ключевых точках здания для обеспечения безопасности и ограниченного доступа (рисунок 3).

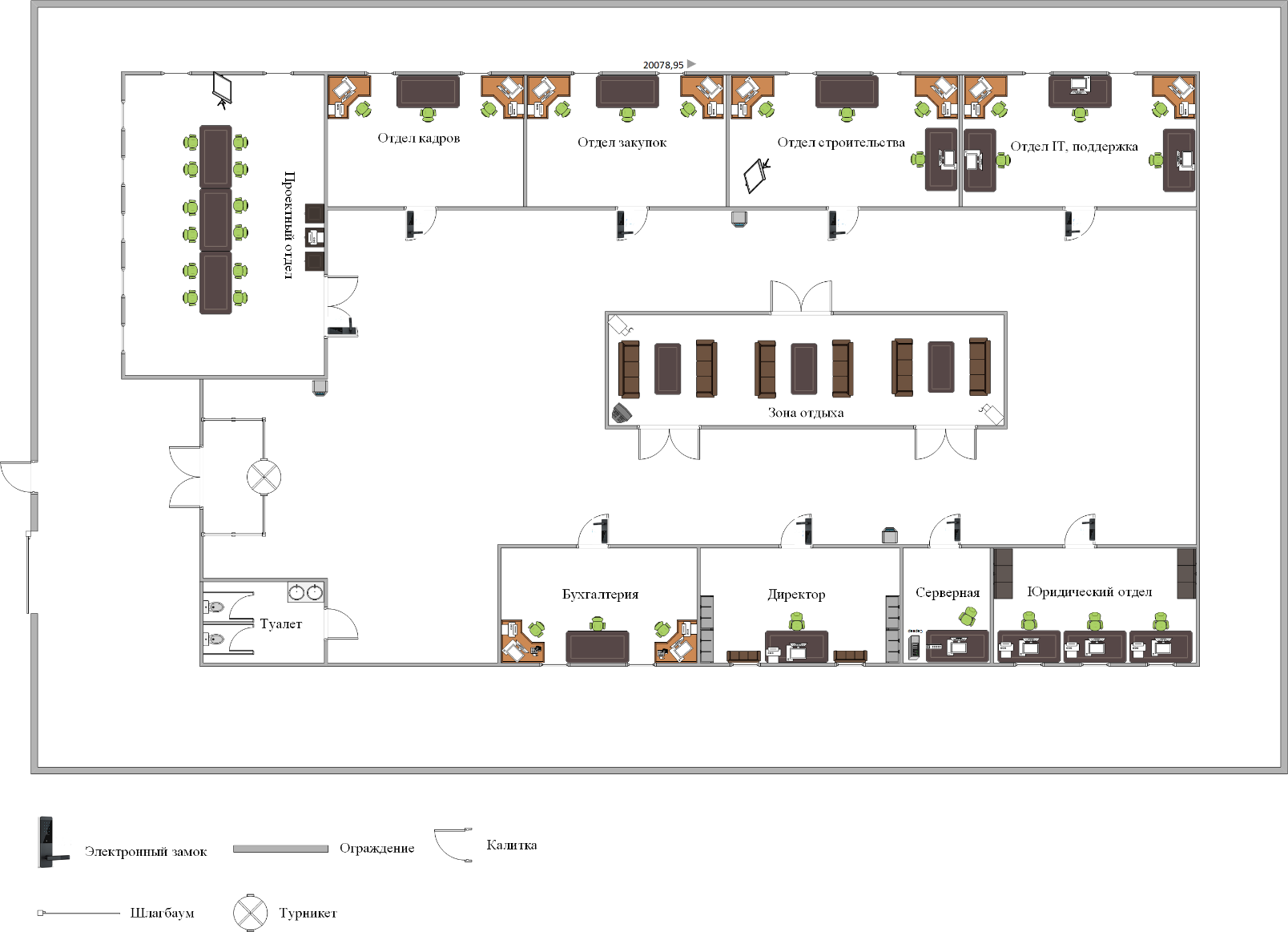


Рисунок 3 – Схема запирающих средств

В условиях постоянно развивающихся технологий безопасности, электронные дверные замки представляют собой важный компонент системы защиты объектов, включая предприятия строительной сферы, вроде компании "Калуга-Стройдом". Эти замки предлагают ряд преимуществ перед традиционными механическими замками, такими как удобство использования, повышенный уровень безопасности и возможность интеграции с другими системами безопасности.

Одним из ключевых преимуществ электронных дверных замков является их уникальная система доступа. Они позволяют предоставлять доступ к помещениям посредством использования различных методов аутентификации, таких как пин-коды, биометрические сканеры отпечатков пальцев или даже мобильные приложения. Это обеспечивает более высокий уровень безопасности, поскольку ключи или карты доступа могут быть потеряны или украдены, в то время как уникальные биометрические данные или персональные пин-коды сложнее подделать или украсть.

Кроме того, электронные замки обладают дополнительными функциями, такими как возможность ведения журнала доступа, автоматическая блокировка после нескольких неудачных попыток ввода кода, а также интеграция с системами видеонаблюдения и управления доступом. Это позволяет управлять доступом к помещениям более эффективно и безопасно.

Дверные замки Private Vescona (модель RX-2039-T) представляют собой современные электронные замки, которые обеспечивают высокий уровень безопасности и удобства использования. Эти замки предназначены для использования в коммерческих и жилых помещениях, включая офисы, гостиницы, апартаменты и дома.

Электронный замок Private Vescona был использован для обеспечения безопасности и контроля доступа в помещения компании (рисунок 4).



Рисунок 4 – Электронный замок Private Vescona

Одной из ключевых особенностей замков Private Vescona является их многофункциональность. Они обеспечивают различные способы доступа, такие как механический ключ, пин-код, бесконтактные карты доступа и даже биометрическое распознавание отпечатков пальцев. Это позволяет пользователям выбирать наиболее удобный и безопасный способ входа в помещение.

Кроме того, замки Private Vescona обладают продвинутыми функциями безопасности. Они могут записывать журнал доступа, что позволяет вести контроль за временем и лицами, получающими доступ к помещению. Также эти замки могут быть интегрированы с другими системами безопасности, такими как системы видеонаблюдения и мониторинга доступа.

Одной из главных преимуществ замков Private Vescona является их надежность и долговечность. Изготовленные из высококачественных материалов, они обеспечивают долгий срок службы и защиту от несанкционированного доступа.

Таблица 1. Характеристика электронного замка Private Vescona

|  |  |  |
| --- | --- | --- |
| Характеристика | | Значение |
| Размеры ручек | | Внешняя - 160х295х70 мм  Внутренняя - 160х295х70 мм |
| Питание | | Батарейки АА – 4 шт. |
| Приложение | | TTHotel, TTLock |
| Габариты упаковки | | 350/200/120мм |
| Торговая марка | | «Private» |
| Назначение устройства | | Автоматизация отелей |
| Питание | Допустимое напряжение | 4,2 - 6 В |
| Максимальное потребление | 0,036 Вт |
| Тип подключения | Автономный (без подключения) |
| Класс защищенности | | III |
| Режим работы | | Непрерывно |
| Время работы под нагрузкой | | Длительное |
| Степень защиты корпуса | | IP30 |
| Инсталляция | | Двери межкомнатные и входные |
| Реакция на сбой питания | | Сохранение данных согласно параметризации |
| Реакция на восстановление питания | | Восстановление данных согласно параметризации |
| Индикация режимов работы | | LED зеленым – команда принята, LED красный – ошибка ввода |
| Материал корпуса | | Алюминий – литье под давлением, SUS304 |

Карточка доступа для электронного замка — это электронный ключ, предоставляющий доступ к заблокированным помещениям или объектам. Эти карточки могут использовать различные технологии, такие как RFID (Radio-Frequency Identification), NFC (Near Field Communication), магнитная полоса или бесконтактные микрочипы. Обычно они имеют стандартный размер банковской карточки для удобства ношения и хранения.

Некоторые карточки доступа могут быть программированы для работы с определенными замками или системами доступа, что обеспечивает администраторам легкое управление доступом персонала. Они могут быть защищены паролем или шифрованием для предотвращения несанкционированного доступа.

Карта доступа Em-marine была использована для обеспечения удобного и надежного доступа к защищенным зонам компании (рисунок 5).



Рисунок 5 – Карта доступа Em-marine

Карта доступа толстая Em-marine с прорезью — это тип карточки доступа, используемой для электронных замков и систем контроля доступа. Она оснащена прорезью для удобства крепления к брелокам, бейджам или ключам. Эти карты работают на частоте 125 кГц и используют технологию RFID (Radio-Frequency Identification), позволяющую бесконтактно передавать информацию между карточкой и считывающим устройством.

Таблица 2. Характеристики карты доступа Em-marine

|  |  |
| --- | --- |
| Характеристика | Значение |
| Тип | Карта доступа RFID |
| Модель | Толстая Em-marine (RX-2039-T) |
| Частота | 125 кГц |
| Технология RFID | Clamshell |
| Уникальный код (идентификатор) | Присутствует |
| Поддержка безопасности | Стандартные меры защиты доступа |
| Прочность | Высокая |

Шлагбаум — это устройство, предназначенное для организации и контроля движения транспортных средств на территории организации или объекта. Он состоит из горизонтальной балки (барьера), которая поднимается и опускается для блокировки или открытия проезда, механизма для управления подъемом и опусканием барьера, системы управления, опор и фундамента. Шлагбаумы обеспечивают безопасность и контроль доступа на объект, а также организуют движение транспортных средств, что делает их незаменимым элементом инфраструктуры для различных предприятий и организаций. Они могут быть оснащены различными опциями безопасности для обеспечения надежной и безопасной работы. Выбор конкретной модели шлагбаума зависит от требований и характеристик конкретного объекта, а также от уровня автоматизации и функциональных возможностей, необходимых для решения задач контроля доступа и безопасности.

Шлагбаум CAME Gard 4000 был использован для автоматизированного контроля въезда на территорию компании, обеспечивая надежную защиту и упорядоченный доступ транспортных средств (рисунок 6).



Рисунок 6 – Шлагбаум CAME Gard 4000

CAME Gard 4000 — это автоматический шлагбаум, предназначенный для контроля доступа и организации движения на территории объектов. Он обладает длиной балки 4 метра, что обеспечивает широкие возможности для ограничения проезда транспортных средств различных типов. Шлагбаум оснащен автоматизированным механизмом управления, который позволяет эффективно и быстро поднимать, и опускать балку для блокировки или открытия проезда.

Таблица 3. Характеристики шлагбаума CAME Gard 4000

|  |  |
| --- | --- |
| Характеристика | Заявление |
| Электропитание мотора | 24 В |
| Мощность | 300 Вт |
| Макс. крутящий момент | 200 Нм |
| Время открывания | 2-6 с |
| Класс защиты | IP54 |

Калитка — это небольшая дверь или ворота, которые предназначены для прохода пешеходов через ограждение. Она является частью общей системы безопасности и управления доступом на территорию объекта (рисунок 7).



Рисунок 7 - Калитка распашная с панелью

Турникеты — это средства контроля доступа, которые широко применяются в различных общественных и коммерческих зданиях для регулирования потока людей. Они обеспечивают контроль за проходом через определенные точки входа или выхода, обеспечивая безопасность и ограничивая доступ только авторизованным лицам.

Основная функция турникета — это поворотные элементы, которые могут быть механическими или электронными. Механические турникеты могут иметь вертушки или барьеры, которые вращаются или поднимаются при проходе авторизованного лица. Электронные турникеты обычно оснащены электроприводом, который управляет открытием и закрытием барьеров.

Считыватели доступа - еще один важный элемент турникета. Они предназначены для считывания и проверки идентификационных карточек, брелоков, биометрических данных или других устройств доступа, которые предоставляются пользователям для прохождения через турникет.

Системы управления обеспечивают работу турникета и его взаимодействие с системой контроля доступа. Они включают в себя электронные платы, моторы и другие компоненты, которые обеспечивают автоматизацию работы турникета и интеграцию его с общей системой безопасности.

Турникет "Ростов-Дон Т9М1-02" был использован для автоматизированного контроля доступа сотрудников и посетителей, обеспечивая надежную защиту и упорядоченный проход на территорию компании (рисунок 8).



Рисунок 8 - Турникет "Ростов-Дон Т9М1-02"

Турникет "Ростов-Дон Т9М1-02" представляет собой современное средство контроля доступа, которое активно применяется для обеспечения безопасности и регулирования потока людей в различных организациях, аэропортах, стадионах, банках и других общественных местах.

Таблица 4. Характеристики турникета "Ростов-Дон Т9М1-02"

|  |  |
| --- | --- |
| Характеристика | Значение |
| Напряжение питания турникета | 12±2 B постоянного тока |
| Стыковка со СКУД | Любые типы СКУД |
| Пропускная способность в режиме однократного прохода | 30-40 чел./мин. |
| Средняя наработка на отказ, проходов | 2 000 000 |
| Срок эксплуатации, не менее | 8 лет |

В результате проведенного анализа и изучения доступных запирающих средств и систем для организации физической защиты, были выделены несколько ключевых моментов.

Во-первых, выбор запирающих средств и систем должен основываться на конкретных потребностях и требованиях организации, учитывая особенности её деятельности и уровень защиты, необходимый для обеспечения безопасности персонала и имущества.

Во-вторых, важно учитывать степень защиты, надежность и функциональность выбранных средств, а также их совместимость с другими системами безопасности, такими как системы контроля доступа и видеонаблюдения.

Также следует обратить внимание на возможность дальнейшего расширения и модернизации системы запирания для адаптации к изменяющимся потребностям организации и среды.

Наконец, важно обеспечить обучение персонала по правилам и процедурам использования запирающих средств и систем, а также поддержку и обслуживание оборудования для обеспечения его бесперебойной работы.

В целом, правильный выбор запирающих средств и систем играет ключевую роль в обеспечении безопасности и защите организации от нежелательного доступа и инцидентов, и может значительно повысить уровень защиты и эффективность деятельности организации.

# 2.1.2. Выбор средств видеонаблюдения

При выборе средств видеонаблюдения для обеспечения безопасности и контроля в организации, необходимо учитывать ряд ключевых факторов и требований.

Затем производится обзор доступных на рынке видов видеонаблюдения, их характеристик и особенностей применения. В этом контексте рассматриваются как традиционные аналоговые системы, так и современные цифровые видеокамеры, системы IP-видеонаблюдения, облачные решения и т.д. Особое внимание уделяется техническим характеристикам, таким как разрешение, угол обзора, возможности ночного видения, а также функциональным возможностям, включая детекцию движения, запись видео в реальном времени и удаленный доступ к системе.

Описание схемы здания со средствами видеонаблюдения включает размещение камер видеонаблюдения в ключевых точках для обеспечения максимальной безопасности и контроля (рисунок 9).

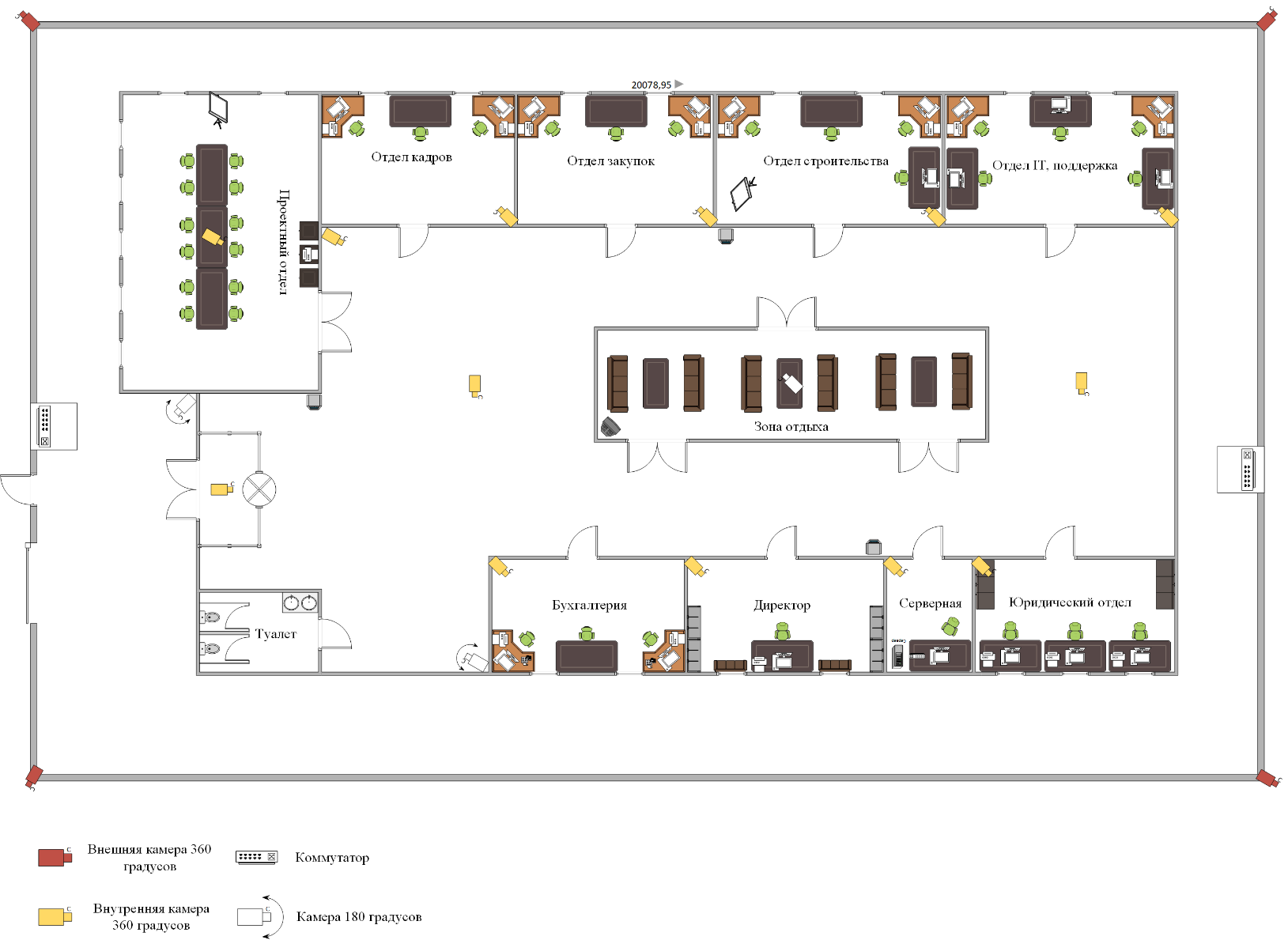


Рисунок 9 – Схема расположения камер видеонаблюдения

Видеокамеры с обзором 360 градусов — это передовые системы видеонаблюдения, способные осуществлять мониторинг больших пространств без слепых зон. Они представляют собой компактные устройства, способные обеспечить обзор вокруг своей оси на 360 градусов без необходимости установки нескольких камер.

Основными характеристиками таких камер являются их угол обзора, разрешение, наличие ночного видения и функции аналитики. Угол обзора до 360 градусов позволяет захватывать изображения сразу со всех сторон, что делает их идеальным решением для наблюдения за большими пространствами, такими как склады, паркинги, торговые залы и другие общественные места.

Высокое разрешение видеокамер обеспечивает четкое изображение даже на больших расстояниях, а наличие инфракрасной подсветки позволяет осуществлять наблюдение в темное время суток. Некоторые модели обладают расширенными функциями аналитики, такими как детекция движения, распознавание лиц и автоматическое отслеживание объектов, что повышает эффективность системы наблюдения.

Управление параметрами камер и доступ к видеопотокам может осуществляться как локально, через специальное программное обеспечение, так и удаленно, через сеть Интернет.

Эти камеры широко применяются в областях общественной безопасности, мониторинга производственных процессов, наблюдения за общественными местами и других сферах, где требуется обеспечение всестороннего и эффективного видеонаблюдения.

Видеокамера TP-Link Tapo C500 была использована для обеспечения всестороннего видеонаблюдения в офисных и производственных помещениях компании, предоставляя высокое качество изображения и широкие возможности мониторинга (рисунок 10).



Рисунок 10 - Видеокамера TP-Link Tapo C500

Видеокамера TP-Link Tapo C500 — это современное устройство видеонаблюдения, предназначенное для обеспечения безопасности офиса или другого помещения. Она обладает рядом характеристик и функций, делающих ее популярным выбором среди потребителей.

Таблица 5. Характеристики видеокамеры TP-Link Tapo C500

|  |  |
| --- | --- |
| Характеристика | Значение |
| Матрица | 1/3 дюйма |
| Разрешение | 1080p Full HD (1920 × 1080 пикселей) |
| Угол обзора | По горизонтали — 360°, по вертикали — 130° |

Продолжение таблицы 5. Характеристики видеокамеры TP-Link Tapo C500

|  |  |
| --- | --- |
| Стандарты и протоколы | IEEE 802.11b/g/n, 2,4 ГГц |
| Протоколы | TCP/IP, ICMP, DNS, HTTPS, TCP, UDP |
| Частота | 2,4 ГГц |
| Стандарты безопасности | WPA/WPA2-PSK |

Видеокамеры с обзором 180 градусов представляют собой компактные и удобные устройства видеонаблюдения, способные охватывать широкую область пространства без потери качества изображения. Они предлагают широкий угол обзора без необходимости установки нескольких камер, что делает их особенно привлекательными для мест, где требуется максимальное покрытие без слепых зон.

Основные характеристики таких камер включают высокое разрешение, качественное изображение на всей площади наблюдения, интеллектуальные функции, такие как детектор движения и звука, а также возможность ночного видения благодаря инфракрасным светодиодам. Кроме того, они обычно поддерживают удаленное управление через мобильные приложения или веб-интерфейс, что обеспечивает удобство в использовании и мониторинге.

Установка и настройка таких камер обычно довольно просты, что делает их доступными для широкого круга пользователей. Они также предлагают возможность хранения записей в облачных сервисах для удобного и надежного хранения видеоматериалов. В целом, видеокамеры с обзором 180 градусов являются эффективным средством видеонаблюдения для различных сфер применения, предлагая широкий функционал и простоту использования.

IP камера Hikvision 1.68мм (DS-2CD2345G0P-I) была использована для обеспечения качественного видеонаблюдения с широким углом обзора в различных зонах компании, способствуя повышению уровня безопасности и контроля (рисунок 11).



Рисунок 11 - IP камера Hikvision 1.68мм (DS-2CD2345G0P-I)

IP-камера Hikvision DS-2CD2345G0P-I представляет собой высококачественное устройство видеонаблюдения, обладающее рядом продвинутых функций и характеристик, которые делают ее привлекательным выбором для различных объектов видеонаблюдения.

Таблица 6. Характеристики IP камеры Hikvision 1.68мм (DS-2CD2345G0P-I)

|  |  |
| --- | --- |
| Характеристика | Значение |
| Размер матрицы | 1/2.7 |
| Тип матрицы | CMOS |
| Макс. угол обзора | 180 |
| Макс. разрешение видеокамеры | 2688x1520 |
| Класс защиты IP | IP67 |
| POE | POE |
| Фокусное расстояние | 1.68 мм |

Уличный навесной шкаф для коммутатора представляет собой специализированное оборудование, предназначенное для защиты сетевого оборудования, такого как коммутаторы, маршрутизаторы и другие устройства, используемые для организации сети на открытом воздухе. Такой шкаф обеспечивает безопасность и надежность работы сетевого оборудования, защищая его от неблагоприятных погодных условий, механических повреждений, пыли и влаги (рисунок 12).



Рисунок 12 - Термошкаф уличный навесной МАСТЕР-3 УТ

Термошкаф уличный навесной "МАСТЕР-3 УТ" — это специализированное оборудование, предназначенное для защиты сетевых коммутаторов и другого сетевого оборудования от неблагоприятных погодных условий и других внешних воздействий при размещении на открытом воздухе. Этот шкаф обеспечивает надежную и безопасную работу сетевого оборудования даже в самых экстремальных климатических условиях.

Таблица 7. Характеристики термошкафа МАСТЕР-3 УТ

|  |  |
| --- | --- |
| Характеристика | Заявление |
| Степень защиты от пыли и влаги | IP 66 |
| Дополнительные функции | Установка на открытом воздухе, замок с ключом |
| Комплектующие | Корпус, розетки |

Коммутатор неуправляемый — это сетевое устройство, которое используется для соединения нескольких устройств в локальной сети (LAN). В отличие от управляемых коммутаторов, неуправляемые коммутаторы не имеют пользовательского интерфейса и функций настройки. Они предоставляют простое и надежное соединение между устройствами, автоматически перенаправляя трафик на основе MAC-адресов (рисунок 13).



Рисунок 13 - Коммутатор TP-LINK TL-SG1005LP

Коммутатор TP-LINK TL-SG1005LP — это неуправляемый сетевой коммутатор, который предназначен для малого и среднего бизнеса. Он оснащен пятью гигабитными портами, поддерживающими технологию PoE+, что делает его идеальным решением для подключения и управления сетевыми устройствами, такими как IP-камеры, точки доступа, телефоны VoIP и другие устройства, требующие питания через Ethernet.

Таблица 8. Характеристики коммутатора TP-LINK TL-SG1005LP

|  |  |
| --- | --- |
| Характеристика | Заявление |
| Количество LAN-портов | 5 |
| Размер таблицы MAC адресов | 2048 |
| Базовая скорость передачи данных | 1 Гбит/с |
| Сетевые стандарты | IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN), IEEE 802.3ab, IEEE 802.3af, IEEE 802.3at, IEEE 802.3u, IEEE 802.3x, IGMP Snooping, IGMP v1, Jumbo Frame, автоопределение MDI/MDIX |

Кабель для подключения IP камер играет ключевую роль в обеспечении передачи данных и питания для камеры (рисунок 14).



Рисунок 14 - Кабель Ethernet для IP камеры видеонаблюдения Onviz

PoE (Power over Ethernet) коммутаторы представляют собой сетевые устройства, которые позволяют передавать как данные, так и электропитание через один и тот же сетевой кабель Ethernet. Это позволяет упростить подключение устройств к сети, особенно в тех случаях, когда доступ к электричеству ограничен или неудобен.

Основная функция PoE коммутаторов - обеспечение питания подключенным устройствам, таким как IP-камеры видеонаблюдения, точки доступа Wi-Fi, VoIP-телефоны и другие сетевые устройства. Это делает их особенно полезными в ситуациях, когда устройства расположены на значительном удалении от источника питания.

PoE коммутаторы могут иметь разное количество портов и различные конфигурации, что обеспечивает гибкость и масштабируемость при проектировании и настройке сети. Они также могут поддерживать различные стандарты PoE, такие как PoE, PoE+, 802.3af и 802.3at, что позволяет выбирать подходящее решение в зависимости от требований конкретного проекта.

Таким образом, PoE коммутаторы являются удобным и эффективным средством для создания сетей связи и видеонаблюдения, обеспечивая простоту установки, гибкость в настройке и экономию затрат на проводку.

PoE коммутатор IPTRONIC PS2-E28P24M был использован для эффективного питания и управления сетевыми устройствами, такими как IP-камеры и точки доступа, что значительно упростило установку и эксплуатацию системы видеонаблюдения (рисунок 15).



Рисунок 15 - PoE коммутатор IPTRONIC PS2-E28P24M

Выбор управляемого PoE коммутатора IPTRONIC PS2-E28P24M обусловлен его впечатляющими характеристиками и возможностями. Этот коммутатор обладает 24 портами с поддержкой PoE, что позволяет подключать и питать через Ethernet множество устройств, включая IP-камеры и точки доступа, без необходимости дополнительного электропитания. Кроме того, наличие 2 портов Gigabit Ethernet и 2 SFP портов расширяет возможности подключения высокоскоростных устройств и обеспечивает высокую производительность сети.

Таблица 9. Характеристики PoE коммутатора IPTRONIC PS2-E28P24M

|  |  |
| --- | --- |
| Характеристика | Описание/Значение |
| Количество портов | 32 |
| Класс POE | 802.3af / 802.3at |
| Скорость передачи данных | 10/100 Мбит/с / 1 Гбит/с |
| Поддержка VPN-тоннелей (VPN Endpoint) | Нет |
| Возможность установить в стойку | Да |

Источник бесперебойного питания (UPS) — это неотъемлемая часть современных информационных и электроэнергетических систем. Он представляет собой устройство, которое обеспечивает непрерывное электропитание при отключении основного источника энергии или при возникновении скачков напряжения в электросети.

Функциональность UPS включает в себя несколько ключевых аспектов. Во-первых, он стабилизирует напряжение, поступающее на подключенное оборудование, предотвращая повреждение от резких изменений напряжения. Во-вторых, в случае отключения основного электропитания, UPS автоматически переключается на свой встроенный источник питания, обеспечивая непрерывную работу оборудования. Кроме того, UPS обычно обладает функцией временного обеспечения электричеством, что дает возможность сохранить данные и корректно завершить работу системы в случае длительного отключения питания.

Важным аспектом работы UPS является защита подключенного оборудования от скачков напряжения и перенапряжений в электросети. UPS фильтрует входящий сигнал, предотвращая повреждения оборудования и обеспечивая его надежную работу.

Современные UPS также оснащены функцией мониторинга состояния батареи и оповещения администратора о необходимости замены или обслуживания. Это позволяет своевременно производить техническое обслуживание и поддерживать эффективную работу системы.

В целом, источники бесперебойного питания играют важную роль в поддержании непрерывности работы информационных и электроэнергетических систем, обеспечивая защиту от сбоев в электроснабжении и сохранение данных.

ИБП APC Back-UPS 650VA 230V AVR Schuko был использован для обеспечения непрерывного питания критически важных систем и защиты оборудования от перебоев в электроснабжении и скачков напряжения, что повысило надежность и стабильность работы всей инфраструктуры (рисунок 16).

Рисунок 16 - ИБП APC Back-UPS 650VA 230V AVR Schuko



Источник бесперебойного питания (ИБП) APC Back-UPS 650VA 230V AVR Schuko является надежным и компактным устройством, предназначенным для обеспечения непрерывного электропитания в случае отключения основного источника энергии или скачков напряжения в электросети.

Таблица 10. Характеристики ИБП APC Back-UPS 650VA 230V AVR Schuko

|  |  |
| --- | --- |
| Характеристика | Значение |
| Номинальная мощность | 325 Вт | 650 ВА |
| Фазы вх. / вых | 1 ф / 1 ф |

Продолжение таблицы 10. Характеристики ИБП APC Back-UPS 650VA 230V AVR Schuko

|  |  |
| --- | --- |
| Тип | line-interactive |
| Габариты | 101x141x300 мм |

Сервер для хранения данных является ключевым компонентом в информационной инфраструктуре компании. Он предназначен для надежного и безопасного хранения больших объемов информации, обеспечивая ее доступность и целостность. Основные характеристики таких серверов включают в себя высокую производительность, надежность и масштабируемость.

Производительность сервера для хранения данных определяется его аппаратными характеристиками, такими как процессор, оперативная память и накопители данных. Он должен быть способен эффективно обрабатывать запросы на доступ к информации и обеспечивать высокую скорость передачи данных.

Надежность является одним из ключевых качеств серверов для хранения данных. Они обычно оснащены резервированными блоками питания и RAID-массивами, которые обеспечивают защиту данных от потери в случае сбоя оборудования или сбоя в работе системы.

Масштабируемость серверов для хранения данных позволяет им адаптироваться к изменяющимся потребностям компании и увеличивать емкость хранения информации по мере необходимости.

Управление данными на сервере для хранения данных осуществляется с помощью специализированных программных средств, которые обеспечивают создание, организацию и защиту информации. Эти средства позволяют администраторам контролировать доступ к данным, резервное копирование и восстановление информации в случае необходимости.

Сервер Dell PowerEdge R630 8SFF использовался для обеспечения надежного и масштабируемого хранения данных в информационной системе компании (рисунок 17).

Рисунок 17 – Сервер Dell R630 8SFF



Сервер Dell PowerEdge R630 8SFF — это высокопроизводительное решение, предназначенное для обработки данных и выполнения различных вычислительных задач в средних и крупных корпоративных сетях. Он отличается компактным дизайном и высокой производительностью, что делает его идеальным выбором для масштабирования и оптимизации ИТ-инфраструктуры компаний.

Таблица 11. Характеристика сервера Dell R630 8SFF

|  |  |
| --- | --- |
| Характеристика | Значение |
| Процессор | До 2 процессоров Intel Xeon E5-2600 v4, до 22 ядер на процессор |
| Охлаждение | Воздушное |
| Форм-фактор | 1U rack |
| Память | До 24 слотов для модулей памяти ECC DDR4 DIMM, максимум 1.5 ТБ, максимальная скорость 2400 миллионов транзакций в секунду |
| Безопасность | Защелка крышки, TPM, Безопасность при отключении питания, Оповещение о вторжении, Безопасный режим |
| Слоты PCI-e | До 3 слотов PCIe 3.0 + выделенный слот платы RAID |
| Вентиляторы | До 7 стандартных вентиляторов |

В заключении этого раздела можно отметить, что выбор средств видеонаблюдения для строительной компании "Калуга-Стройдом" имеет важное стратегическое значение для обеспечения безопасности объектов, контроля рабочих процессов и улучшения оперативности реагирования на потенциальные угрозы и происшествия.

Анализ рынка видеонаблюдения позволил выявить различные модели камер, включая видеокамеры 360 градусов, видеокамеры 180 градусов, а также IP камеры различных производителей, таких как Hikvision и TP-Link. Каждая из этих камер обладает своими особенностями, преимуществами и областями применения.

В ходе выбора средств видеонаблюдения были учтены требования по различным параметрам, таким как разрешение видео, угол обзора, возможности ночного видения, поддержка стандартов сжатия видео, а также совместимость с другими системами безопасности.

Таким образом, выбор оптимальных средств видеонаблюдения с учетом всех указанных параметров позволит обеспечить эффективное и надежное функционирование системы безопасности на объектах строительной компании "Калуга-Стройдом", повысить уровень безопасности и контроля, а также обеспечить сохранность имущества и персонала.

# 2.1.3. Выбор средств пожарно-охранной сигнализации

В современном мире безопасность является одним из приоритетных аспектов в управлении любой организацией. Строительная компания "Калуга-Стройдом" стремится обеспечить безопасность своих объектов и персонала на высоком уровне. В этом контексте важным элементом является выбор средств пожарно-охранной сигнализации, которые не только обеспечат раннее обнаружение и быстрое реагирование на пожары, но и помогут предотвратить потери и минимизировать риски для жизни и здоровья работников.

Цель данного исследования заключается в выборе оптимальных средств пожарно-охранной сигнализации для строительной компании "Калуга-Стройдом", которые соответствуют ее потребностям, обеспечивают надежную защиту от пожаров и обеспечивают безопасность на объектах (рисунок 18).

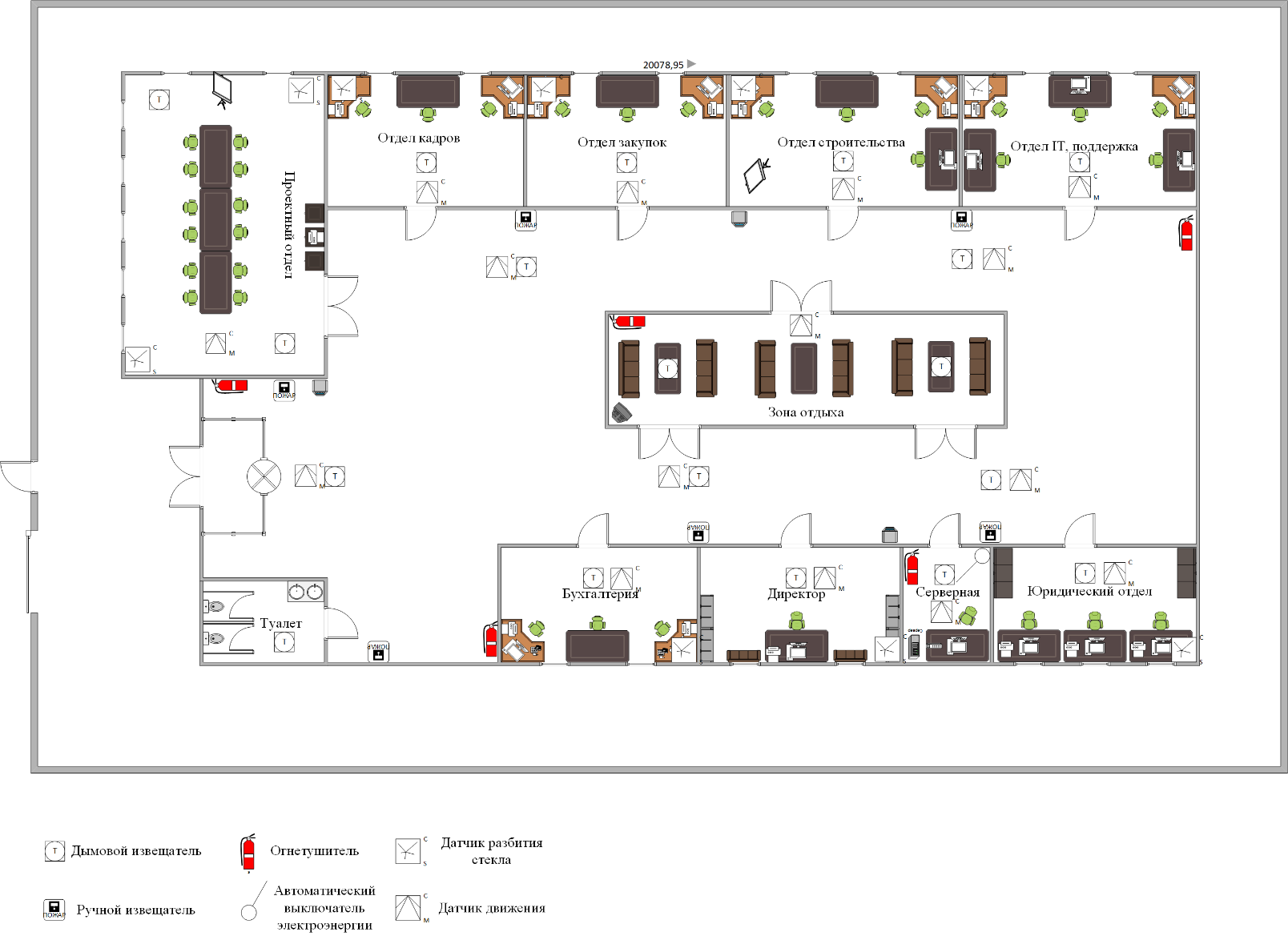


Рисунок 18 – Схема пожарно-охранной сигнализации

Огнетушитель — это специальное устройство, предназначенное для тушения возгораний. Оно играет важную роль в системе пожарной безопасности, позволяя быстро и эффективно локализовать, и потушить начальный очаг возгорания до прибытия пожарной службы.

Огнетушители должны регулярно проходить техническое обслуживание и проверки на годность к использованию. Обучение персонала правилам эксплуатации огнетушителей также является важной составляющей обеспечения пожарной безопасности на объектах строительной компании.

Огнетушитель ОП-4(з)-АВСЕ-01 был использован для обеспечения первичной пожарной безопасности на объекте, что позволило оперативно реагировать на возгорания и минимизировать потенциальные убытки и угрозы для жизни и здоровья сотрудников (рисунок 19).



Рисунок 19 – Огнетушитель ОП-4(з)-АВСЕ-01

Огнетушитель ОП-4(з)-АВСЕ-01 (4 кг) металл — это порошковый огнетушитель, предназначенный для тушения различных классов пожаров. Он характеризуется высокой эффективностью и простотой в использовании, что делает его идеальным выбором для обеспечения пожарной безопасности на объектах строительной компании "Калуга-Стройдом".

Огнетушитель ОП-4(з)-АВСЕ-01 имеет массу в 4 кг, что обеспечивает достаточное количество порошка для тушения небольших пожаров. Он оснащен манометром, который позволяет контролировать давление внутри баллона и обеспечивать надежность работы огнетушителя.

Металлическое исполнение огнетушителя обеспечивает его долговечность и стойкость к механическим воздействиям, что особенно важно в условиях строительных объектов. Закачной механизм упрощает процесс подготовки огнетушителя к использованию и обеспечивает возможность быстрой замены или дозаправки порошка после использования.

Огнетушитель упакован в гофрокороб, что обеспечивает его защиту от повреждений и удобство транспортировки и хранения. Важно помнить, что для эффективного использования огнетушителя необходимо обеспечить обучение персонала правилам его эксплуатации и проведение регулярных проверок на годность к использованию.

Таблица 12. Характеристики огнетушителя ОП-4(з)-АВСЕ-01

|  |  |
| --- | --- |
| Характеристика | Значение |
| Тип огнетушителя | Порошковый |
| Класс пожара | A, B, C, E, ABCE, А/В/С/Е, АВСЕ |
| Объем заряда | 5 л |

Продолжение таблицы 12. Характеристики огнетушителя ОП-4(з)-АВСЕ-01

|  |  |
| --- | --- |
| Тип пускового устройства | Рычажного типа |
| Способ срабатывания | Ручной |

Извещатель пожарный дымовой — это устройство, предназначенное для обнаружения дыма, возникающего в результате пожара. Его основная задача - раннее оповещение о возможном возгорании для обеспечения безопасной эвакуации людей и защиты имущества. Обычно такие извещатели устанавливаются в помещениях, где есть риск пожара, например, в квартирах, офисах, складах и производственных помещениях.

Когда датчик обнаруживает дым, извещатель срабатывает и активирует сигнал оповещения. Это может быть звуковой сигнал, световой сигнал или комбинация обоих. Извещатели пожарной сигнализации часто подключаются к центральной панели управления, что позволяет оперативно реагировать на пожарную тревогу и принимать необходимые меры по тушению пожара или эвакуации людей.

Извещатель пожарный дымовой автономный ИП 212-50М2 был использован для обеспечения раннего обнаружения дыма и предупреждения о возможных пожарах, что позволяет оперативно принимать меры по эвакуации и ликвидации возгорания, обеспечивая безопасность людей и сохранность имущества (рисунок 20).



Рисунок 20 - Извещатель пожарный дымовой автономный

ИП 212-50М2

Извещатель пожарный дымовой автономный ИП 212-50М2 — это автономное устройство, предназначенное для обнаружения дыма, возникающего при пожаре, без привязки к центральной пожарной сигнализации. Он обеспечивает раннее обнаружение возгорания в помещениях и автоматическое оповещение о пожаре.

Таблица 13. Характеристики пожарного извещателя ИП 212-50М2

|  |  |
| --- | --- |
| Характеристика | Значение |
| Тип извещателя | Дымовой |
| Монтаж | На потолок/стену |
| Звуковой сигнал | Да, встроенный |
| Степень защиты | IP20 (защита от пыли) |
| Срок службы батарей/аккумуляторов | Не менее 1 года |
| Назначение | Пожарное обнаружение |

Пожарные извещатели ручные — это важные компоненты систем пожарной сигнализации, предназначенные для оперативного оповещения о возможном возгорании или других чрезвычайных ситуациях.

Обычно они представляют собой компактные устройства с кнопкой активации, которые могут быть легко нажаты для сигнализации о пожаре. После активации извещатель может включать светодиодные индикаторы или издавать звуковой сигнал, предупреждая окружающих о пожарной угрозе.

Надежность и эффективность таких устройств крайне важны, поэтому они должны быть тщательно протестированы и сертифицированы в соответствии с соответствующими стандартами безопасности.

Извещатель пожарный ручной адресный Болид ИПР 513-3АМ был использован в системе пожарной сигнализации для обеспечения безопасности в помещениях строительной компании "Калуга-Стройдом" (рисунок 21).

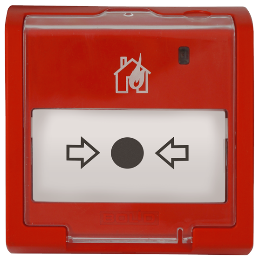


Рисунок 21 - Извещатель пожарный ручной адресный Болид ИПР 513-3АМ

Извещатель пожарный ручной адресный Болид ИПР 513-3АМ представляет собой важное устройство в системе пожарной сигнализации, предназначенное для оперативного обнаружения и оповещения о возможном возгорании или других чрезвычайных ситуациях.

Этот извещатель оснащен кнопкой активации, которая при активации сигнализирует о пожаре. Он также обладает возможностью адресации, что позволяет точно указывать место срабатывания устройства в системе, упрощая локализацию возгорания и оперативное реагирование на него.

Установка извещателя производится на стене или другой доступной поверхности на уровне, удобном для пользователя.

Таблица 14. Характеристики пожарного извещателя ручного Болид ИПР 513-3АМ

|  |  |
| --- | --- |
| Характеристика | Значение |
| Принцип работы извещателя | Оптико-электронный |
| Принцип обнаружения | Точечный |
| Первичный источник тока | Питание от сети |
| Способ монтажа | Накладн. на поверхность |
| Степень защиты | IP40 |
| Тип питающего напряжения | AC (перемен.) |
| Тип пожарного извещателя | Ручной |

Аварийный отключатель электроэнергии — это устройство, предназначенное для автоматического отключения электрического оборудования при возникновении определенных аварийных ситуаций, таких как короткое замыкание, перегрузка или обнаружение пожара.

Принцип работы аварийного отключателя основан на мониторинге параметров электрической сети и автоматическом отключении энергоподачи в случае обнаружения опасных ситуаций. Это может быть достигнуто с помощью различных типов защитных устройств, таких как предохранители, выключатели с дифференциальным током (УЗО), защитные автоматические выключатели (автоматы), а также специализированные устройства для обнаружения пожара.

КПУ11-16/11 (реверс) TDM был использован для аварийного отключения электропитания в случае возникновения пожара (рисунок 22).



Рисунок 22 - КПУ11-16/11 (реверс) TDM

КПУ11-16/11 (реверс) TDM — это устройство, предназначенное для управления и коммутации электрической нагрузки. Оно разработано компанией TDM Electric, которая зарекомендовала себя как надежный производитель электротехнической продукции.

Таблица 15. Характеристики КПУ11-16/11 (реверс) TDM

|  |  |
| --- | --- |
| Характеристика | Значение |
| Тип | Выключатель нагрузки |
| Номинальный ток | 16 А |
| Степень защиты | IP54 |

Датчик разбития стекла – это важное устройство в системе охранной сигнализации, предназначенное для обнаружения разрушения или повреждения стеклянных поверхностей. Разработанный на основе анализа звуковых волн, возникающих при ударе по стеклу, этот датчик активирует тревожный сигнал при обнаружении характерных звуков.

Основная функция датчика заключается в обнаружении специфических звуков, которые возникают при разрушении стекла. Это позволяет быстро и эффективно реагировать на попытки вторжения или повреждения собственности.

DS-PDPG12P-EG2-WE PIR датчик беспроводной с функцией детекции разбития стекла был внедрен в систему безопасности строительной компании "Калуга-Стройдом" для обеспечения надежного контроля за объектами и предотвращения возможных инцидентов (рисунок 23).



Рисунок 23 - DS-PDPG12P-EG2-WE PIR датчик беспроводной с детекцией разбития стекла

DS-PDPG12P-EG2-WE – это беспроводной PIR-датчик с детекцией разбития стекла, который предназначен для обеспечения безопасности помещений.

Таблица 16. Характеристики датчика разбития стекла DS-PDPG12P-EG2-WE PIR

|  |  |
| --- | --- |
| Характеристика | Значение |

Продолжение таблицы 16. Характеристики датчика разбития стекла DS-PDPG12P-EG2-WE PIR

|  |  |
| --- | --- |
| Угол детекции | 85.9° |
| Скорость обнаружения | От 0.3 до 2 м/с |
| Чувствительность разбития стекла | 2 м, 4 м, 6 м, 8 м |
| Тип стекла | Термополированное, листовое, закаленное, армированное |
| Частота передачи | 868 МГц |
| Безопасность передачи данных | Шифрование AES-128 |
| Метод установки | На стену |

Датчики движения — это устройства, которые реагируют на движущиеся объекты в определенной зоне и передают сигнал о их обнаружении. Они широко применяются в системах безопасности и автоматизации, обеспечивая надежное и быстрое обнаружение движения.

Датчики движения используются для активации систем охранной сигнализации, автоматического освещения, управления климатом и других устройств. В зависимости от конкретных потребностей и условий эксплуатации выбираются соответствующие типы и модели датчиков движения.

ИК датчик движения потолочный был внедрен в систему безопасности строительной компании "Калуга-Стройдом" с целью обеспечения контроля за доступом и безопасностью внутри зданий (рисунок 24).



Рисунок 24 - ИК датчик движения ДДТ-01 точечный

Инфракрасный (ИК) датчик движения потолочного типа — это устройство, предназначенное для обнаружения движения в помещении путем регистрации инфракрасного излучения, испускаемого тепловыми источниками, такими как человек или животное. Эти датчики устанавливаются на потолке и обеспечивают широкий угол обзора помещения.

Таблица 17. Характеристики ИК датчика движения

|  |  |
| --- | --- |
| Характеристика | Значение |
| Схема подключения выключателя | Альтернативный переключатель |
| Монтаж | Накладной |
| Ориентация монтажа | Горизонтальная и вертикальная |
| Тип напряжения | Переменный ток (AC) |
| Класс защиты | IP20 |
| Коммутируем. мощность | 1200 Вт |
| Тип | Датчик движения |

Проведенный анализ позволил определить оптимальный набор средств пожарно-охранной сигнализации для обеспечения безопасности объекта. Выбор конкретных устройств осуществлялся с учетом требований к безопасности, особенностей помещений и структуры объекта.

В результате анализа представленного рынка и технических характеристик различных устройств было принято решение в пользу определенных моделей датчиков дыма, датчиков движения, пожарных извещателей и других компонентов системы.

Выбранные средства обладают высокой надежностью, эффективностью и соответствуют современным стандартам безопасности. Они обеспечивают своевременное и надежное обнаружение пожара или вторжения, что позволяет минимизировать риски для жизни и здоровья людей, а также сохранить материальные ценности.

# 2.2. Организация информационной защиты

В данном разделе будет представлен анализ и организация системы информационной защиты для обеспечения безопасности данных и информационных ресурсов строительной компании "Калуга-Стройдом". Организация информационной защиты является важным аспектом для предотвращения утечек конфиденциальной информации, защиты от внешних и внутренних угроз, а также обеспечения непрерывности бизнес-процессов.

На основе результатов анализа будет разработана система информационной защиты, которая включает в себя как технические, так и организационные меры. Будут определены средства ограничения программной среды, меры контроля доступа к информационным ресурсам, а также процессы мониторинга и обнаружения инцидентов информационной безопасности.

Важным этапом организации информационной защиты будет проведение обучения персонала по правилам и процедурам обработки информации, а также по мерам предотвращения угроз информационной безопасности. Это поможет повысить осведомленность сотрудников компании о важности обеспечения безопасности данных.

Особое внимание будет уделено обеспечению непрерывности бизнес-процессов в случае возникновения инцидентов информационной безопасности. Планируется разработка планов восстановления после инцидентов и проведение регулярных тренировок и проверок для повышения готовности к непредвиденным ситуациям.

В результате реализации организации информационной защиты компании "Калуга-Стройдом" ожидается улучшение уровня защиты информации, снижение рисков утечек данных и угроз информационной безопасности, а также обеспечение стабильной и безопасной работы информационных систем компании.

# 2.2.1. Описание информационной среды строительной компании

В современном мире информационные технологии играют ключевую роль в деятельности любого предприятия, в том числе и строительной компании. Понимание информационной среды данного предприятия является необходимым шагом для эффективной организации и управления его информационными ресурсами.

В данном разделе представлено описание информационной среды строительной компании, включая аппаратное и программное обеспечение, сетевую инфраструктуру. Рассмотрение структуры и характеристик информационной среды позволит лучше понять ее особенности и обеспечить безопасное и эффективное функционирование компании.

Серверы:

* сервер хранения данных: Dell R630 8SFF;
* сервер баз данных: Microsoft SQL Server.

Рабочие станции:

* компьютеры персонала: Dell OptiPlex 5070;
* рабочие станции для инженеров и архитекторов: HP ZBook Studio G7.

Сетевое оборудование:

* маршрутизатор: Mikrotik RB4011IGS+RM;
* коммутаторы: IPTRONIC PS2-E28P24M.

Программное обеспечение:

* операционные системы: Windows Server 2019, Windows 10 Pro;
* прикладное ПО: AutoCAD, Revit, Primavera P6, SAP ERP.

Системы хранения данных:

* сетевое хранилище: Synology DiskStation DS423+ для хранения проектных файлов.

Каналы связи и Интернет-подключение:

* локальная сеть (LAN): Ethernet кабели Cat6e;
* широкополосная сеть (WAN): Подключение к интернету через поставщика услуг Интернета.

Описание информационной среды строительной компании позволяет оценить ее текущее состояние и потребности в развитии информационных технологий. Разбор аппаратного и программного обеспечения, анализ сетевой инфраструктуры и систем защиты информации выявляет сильные и слабые стороны текущей информационной среды.

Создание надежной и эффективной сети для строительной компании включает несколько ключевых компонентов, которые обеспечивают бесперебойную работу всех IT-систем и устройств. Ниже приведена схема сети строительной компании с конкретными примерами устройств и их функциями (рисунок 25).

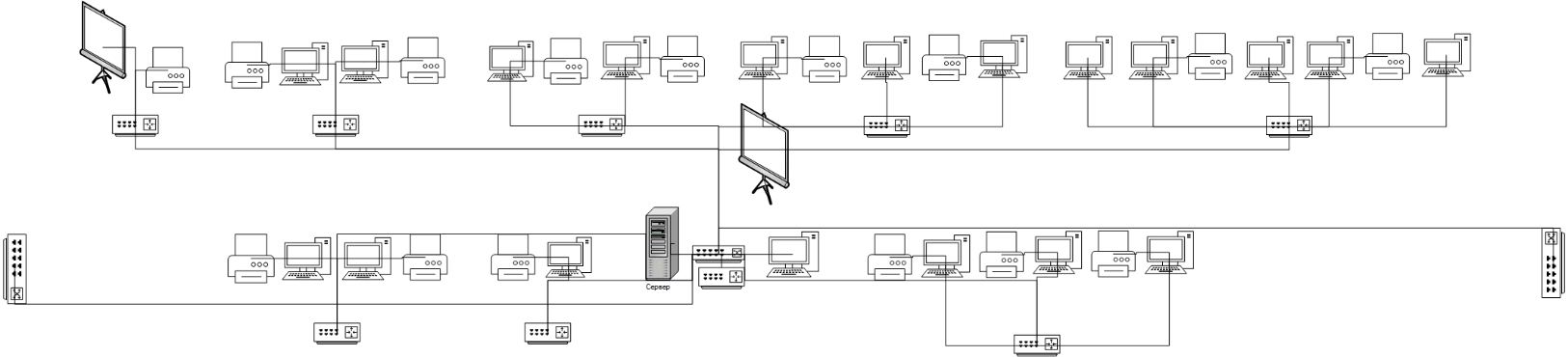


Рисунок 25 – Схема сети строительной компании

Маршрутизатор (или роутер) — это устройство, которое передает пакеты данных между компьютерными сетями, направляя их по оптимальному маршруту. Он не только соединяет сети, но и обеспечивает их безопасность, управляя доступом и предотвращая несанкционированные подключения. Маршрутизаторы могут работать на различных уровнях сети, начиная от домашних и заканчивая крупными корпоративными сетями (рисунок 26).



Рисунок 26 - Wi-Fi роутер MikroTik RB4011iGS+5HacQ2HnD-IN

MikroTik RB4011iGS+5HacQ2HnD-IN — это высокопроизводительный Wi-Fi роутер, который оснащен десятью гигабитными Ethernet-портами, одним портом 10G SFP+ и поддержкой двухдиапазонного Wi-Fi. Этот роутер работает на мощном четырехъядерном процессоре Cortex A15 с тактовой частотой 1,4 ГГц, что обеспечивает высокую производительность и способность обрабатывать большой объем трафика.

Таблица 18. Характеристики Wi-Fi роутер MikroTik RB4011iGS+5HacQ2HnD-IN

|  |  |
| --- | --- |
| Характеристика | Значение |
| Процессор | 1.4 ГГц |

Продолжение таблицы 18. Характеристики Wi-Fi роутер MikroTik RB4011iGS+5HacQ2HnD-IN

|  |  |
| --- | --- |
| Тип подключения | Ethernet + SFP |
| Стандарт Wi-Fi | 4 (802.11n), 5 (802.11ac) |
| Скорость передачи по проводному подключению | 1000 Мбит/с |
| Класс Wi-Fi | AC2000 |

На основе этих данных можно разработать стратегию улучшения информационных технологий в компании, внедрить новые решения для повышения производительности, безопасности и эффективности бизнес-процессов. Важно также регулярно обновлять информационную среду, следить за появлением новых технологий и применять их в соответствии с потребностями компании и требованиями рынка.

# 2.2.2. Средства ограничения программной среды в системе защиты информации

Средства ограничения программной среды в системе защиты информации играют ключевую роль в обеспечении безопасности информационных ресурсов предприятия. Этот раздел посвящен анализу и выбору средств, направленных на ограничение доступа к программному обеспечению и данных, а также на контроль их использования.

Целью данного раздела является оценка существующих методов и средств контроля доступа, а также разработка рекомендаций по их оптимальному применению в информационной среде строительной компании "Калуга-Стройдом".

В ходе исследования будет произведен анализ различных аспектов программной среды, включая уровень привилегий пользователей, механизмы аутентификации и авторизации, а также методы защиты от вредоносных программ и внутренних угроз.

На основе проведенного анализа будет предложен набор средств и методов, которые позволят эффективно ограничить доступ к программному обеспечению и обеспечить целостность и конфиденциальность информации.

Active Directory (AD) — это сервис каталога и управления идентификацией, разработанный и предложенный компанией Microsoft для сред сети Windows. Он обеспечивает централизованное управление и контроль доступа к ресурсам в корпоративной сети.

В основе Active Directory лежит иерархическая структура каталога, которая представляет собой организацию объектов, таких как пользователи, компьютеры, группы и ресурсы. Он предоставляет механизмы для хранения, поиска и управления данными, связанными с этими объектами.

Основные возможности Active Directory включают:

* управление учетными записями пользователей и группами. AD позволяет администраторам создавать, изменять и удалять учетные записи пользователей и групп, а также устанавливать различные атрибуты и права доступа для них;
* централизованная аутентификация и авторизация. AD предоставляет механизмы аутентификации, такие как логин и пароль, для проверки подлинности пользователей при доступе к сетевым ресурсам. Он также определяет права доступа пользователей к этим ресурсам на основе их членства в группах и других настройках безопасности;
* групповая политика. Active Directory позволяет администраторам настраивать параметры безопасности и конфигурации для пользователей и компьютеров с помощью групповых политик. Это позволяет обеспечить единые настройки безопасности и поведения для всех устройств в сети;
* интеграция с другими службами и приложениями. AD интегрируется с различными сервисами и приложениями Windows, такими как Exchange Server, SharePoint, Skype for Business и другими. Это обеспечивает единое окружение управления идентификацией и доступом к ресурсам в организации.

Active Directory является основой для организации безопасности и управления доступом в корпоративных сетях Windows и играет ключевую роль в обеспечении безопасности и производительности сетевых операций (рисунок 27).

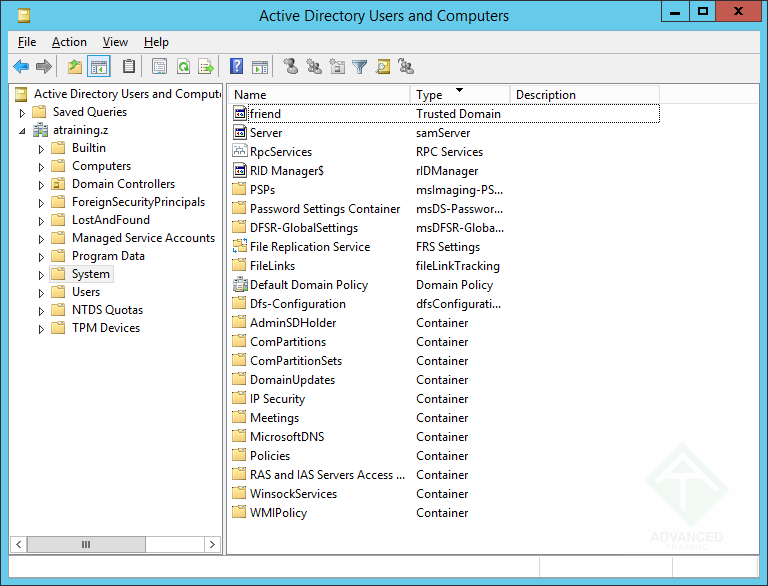


Рисунок 27 – Active Directory

Выбор Active Directory для системы аутентификации и авторизации в строительной компании "Калуга-Стройдом" обусловлен несколькими ключевыми преимуществами, которые делают его оптимальным решением для организации информационной безопасности.

Во-первых, централизованное управление учетными записями пользователей и группами позволяет легко контролировать доступ к корпоративным ресурсам. В компании с большим количеством сотрудников это значительно упрощает процессы создания, изменения и удаления учетных записей, а также управления правами доступа.

Во-вторых, мощные механизмы аутентификации и авторизации обеспечивают высокий уровень безопасности. Использование логинов и паролей, а также возможность интеграции с биометрическими системами аутентификации, позволяют надежно проверять подлинность пользователей при доступе к важным данным и приложениям.

Третье, групповые политики, поддерживаемые Active Directory, дают возможность централизованного управления настройками безопасности и конфигурациями для всех устройств и пользователей в сети. Это обеспечивает единые стандарты безопасности, уменьшает вероятность ошибок и повышает общую защищенность корпоративной сети.

Четвертое, широкая интеграция с другими продуктами и сервисами Microsoft, такими как Exchange Server, SharePoint и Skype for Business, делает Active Directory удобным для комплексного управления IT-инфраструктурой компании. Это способствует более эффективной организации рабочих процессов и взаимодействия между различными службами и подразделениями.

Наконец, надежность и проверенная временем эффективность делают Active Directory стандартом де-факто для управления идентификацией и доступом в корпоративных сетях. Его использование позволяет строительной компании "Калуга-Стройдом" внедрить проверенные и надежные решения для обеспечения безопасности своих информационных ресурсов.

Антивирусное программное обеспечение (ПО) играет ключевую роль в обеспечении безопасности информационной среды любой компании. В строительной компании "Калуга-Стройдом" внедрение надежного антивирусного решения является необходимым шагом для защиты от множества киберугроз, таких как вирусы, трояны, программы-вымогатели, шпионское ПО и другие виды вредоносных программ.

Антивирусное ПО выполняет несколько критически важных функций:

* защита от вредоносных программ. Антивирусное ПО обнаруживает и удаляет вредоносные программы, предотвращая их распространение и минимизируя ущерб;
* мониторинг в реальном времени. Обеспечивает постоянное наблюдение за всеми файлами и приложениями, предотвращая заражение системы;
* защита электронной почты. Проверяет вложения и ссылки в электронных письмах на наличие угроз;
* обнаружение и устранение уязвимостей. Идентифицирует уязвимости в программном обеспечении и системе, предлагая меры по их устранению;
* резервное копирование и восстановление данных. Создает резервные копии данных для предотвращения потерь информации в случае кибератаки.

Kaspersky Endpoint Security for Business — это мощное и надежное антивирусное программное обеспечение, разработанное для защиты корпоративных сетей от различных киберугроз. Оно сочетает в себе передовые технологии защиты и удобные инструменты управления, что делает его идеальным выбором для строительной компании "Калуга-Стройдом" (рисунок 28).

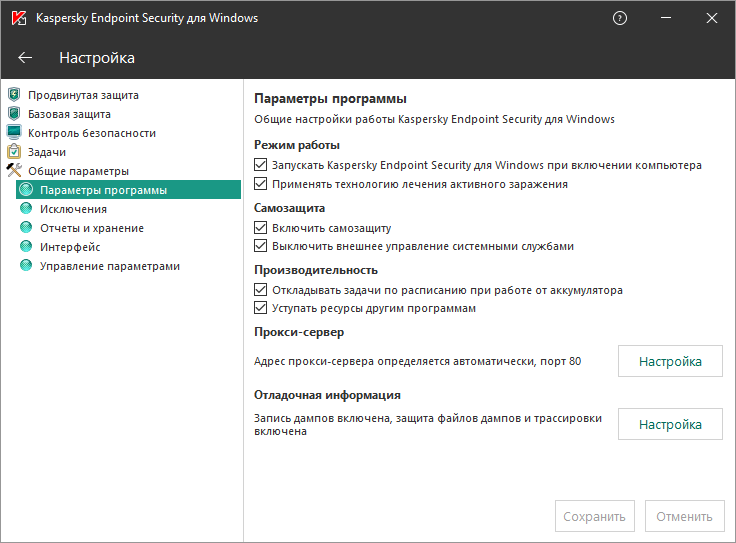


Рисунок 28 - Kaspersky Endpoint Security for Business

Многоуровневая защита:

* антивирусная защита. Обнаруживает и блокирует вредоносные программы, включая вирусы, трояны, черви, шпионское ПО и программы-вымогатели;
* защита от эксплойтов. Предотвращает использование уязвимостей в операционных системах и приложениях;
* проактивная защита. Использует поведенческий анализ и машинное обучение для обнаружения новых и неизвестных угроз.

Мониторинг и контроль:

* мониторинг в реальном времени. Обеспечивает непрерывный контроль за активностью в сети и на рабочих станциях;
* контроль устройств. Управляет доступом к подключаемым устройствам, таким как USB-накопители и внешние жесткие диски, предотвращая несанкционированное копирование данных;
* веб-контроль. Ограничивает доступ к нежелательным и вредоносным веб-ресурсам.

Централизованное управление:

* единый центр управления. Позволяет администраторам управлять защитой всех устройств в сети из одного консоли, упрощая настройку и мониторинг системы безопасности;
* политики безопасности. Позволяет создавать и применять политики безопасности для различных групп пользователей и устройств;
* отчеты и аналитика. Предоставляет подробные отчеты о состоянии безопасности, инцидентах и эффективности мер защиты.

Облачные технологии:

* Kaspersky Security Network (KSN). Использует глобальную облачную сеть для быстрого обнаружения и блокировки новых угроз в реальном времени;
* обновления в реальном времени. Регулярные обновления баз данных сигнатур вирусов и алгоритмов защиты обеспечивают актуальность системы безопасности.

Интеграция и совместимость:

* интеграция с другими системами. Совместимость с популярными операционными системами и программным обеспечением, что позволяет легко интегрировать Kaspersky Endpoint Security в существующую ИТ-инфраструктуру;
* поддержка виртуальных сред. Оптимизировано для работы в виртуальных и облачных средах, обеспечивая высокую производительность и защиту.

Преимущества для компании "Калуга-Стройдом":

* повышение уровня безопасности. Защита от широкого спектра угроз, включая вирусы, программы-вымогатели и шпионское ПО, что минимизирует риски утечек данных и сбоев в работе;
* удобство управления. Централизованная консоль управления и единые политики безопасности упрощают настройку и администрирование системы безопасности;
* экономия времени и ресурсов. Автоматические обновления и проактивная защита снижают нагрузку на ИТ-персонал, позволяя сосредоточиться на основных задачах;
* гибкость и масштабируемость. Возможность адаптации и масштабирования системы безопасности в соответствии с растущими потребностями компании;
* поддержка и обслуживание. Высококачественная техническая поддержка и регулярные обновления обеспечивают надежную защиту и оперативное решение возникающих проблем.

Внедрение Kaspersky Endpoint Security for Business в строительной компании "Калуга-Стройдом" позволит создать надежную и эффективную систему защиты информации. Это обеспечит безопасность корпоративных данных, стабильную работу ИТ-инфраструктуры и защиту от множества киберугроз, что в конечном итоге способствует повышению производительности и защищенности бизнеса.

Межсетевой экран, или фаервол (англ. firewall), представляет собой важное аппаратное или программное решение для защиты компьютерных сетей от несанкционированного доступа и кибератак. Для строительной компании "Калуга-Стройдом" использование межсетевого экрана является критически важным элементом комплексной системы защиты информации.

Основные функции и возможности межсетевого экрана включают контроль доступа, защиту от внешних угроз, сегментацию сети, мониторинг и отчетность, а также интеграцию и управление. Контроль доступа осуществляется через фильтрацию пакетов и управление сессиями, что позволяет разрешать или блокировать пакеты данных в зависимости от заданных правил. Защита от внешних угроз включает превентивную защиту от атак, таких как сканирование портов и DoS-атаки, а также антивирусную защиту, интегрированную в фаервол для обнаружения и блокировки вредоносного ПО в сетевом трафике.

Сегментация сети позволяет разделить физическую сеть на несколько виртуальных сегментов с использованием VLAN, что повышает безопасность и управляемость трафиком. Создание демилитаризованной зоны (DMZ) помогает размещать публичные сервисы, такие как веб-серверы, в отдельной зоне, изолированной от внутренней сети для дополнительной защиты. Мониторинг и отчетность включают ведение подробных журналов всех действий и событий, происходящих на межсетевом экране, а также предоставление аналитики и отчетов о сетевом трафике, инцидентах безопасности и производительности.

Централизованное управление позволяет администрировать несколько межсетевых экранов из единой консоли, что упрощает управление и обновление правил безопасности и сигнатур атак. Регулярные обновления баз данных сигнатур атак и правил безопасности помогают поддерживать актуальный уровень защиты.

Фаервол предотвращает несанкционированный доступ к корпоративным ресурсам, защищает от внешних атак и вредоносного трафика, обеспечивая стабильную и безопасную работу сети. Гибкость и масштабируемость межсетевого экрана позволяют адаптировать и настроить его под конкретные нужды компании и масштабировать по мере роста бизнеса, что снижает риски и повышает общую эффективность работы.

pfSense – это мощное и гибкое открытое и бесплатное программное обеспечение, которое предоставляет множество функций для защиты и управления сетью. Включение pfSense в систему безопасности компании позволит значительно повысить уровень защиты данных и снизить риски кибератак (рисунок 29).

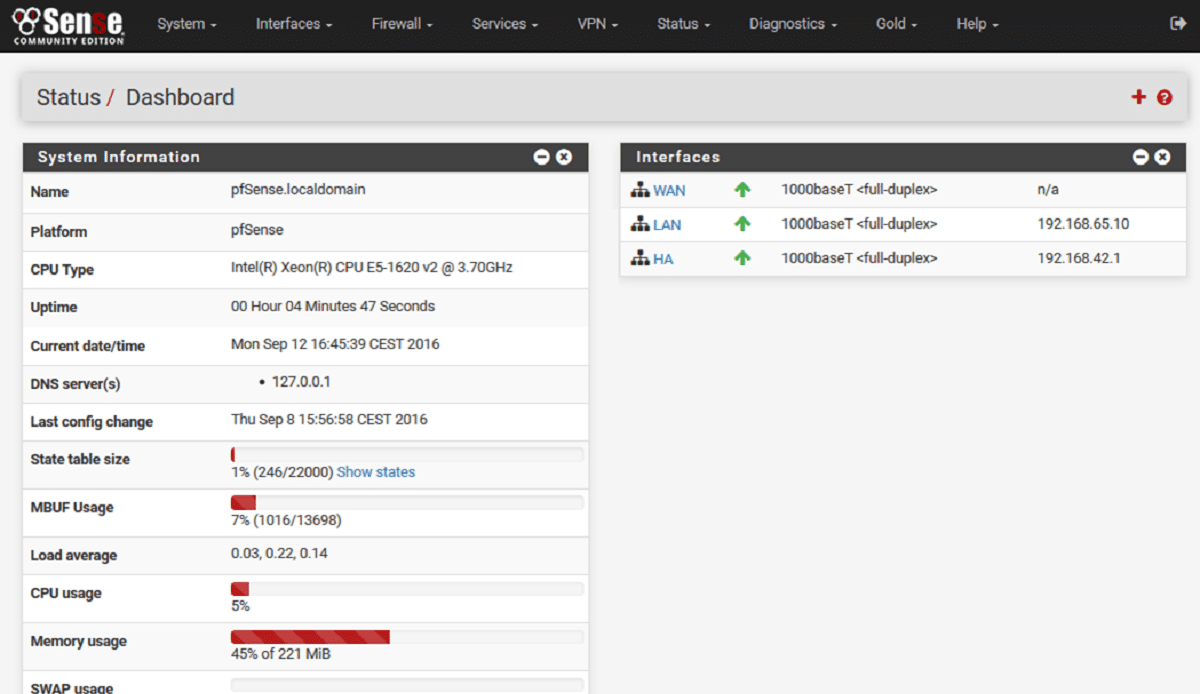


Рисунок 29 – Межсетевой экран pfsense

pfSense обладает рядом ключевых характеристик, которые делают его оптимальным выбором для обеспечения безопасности сети:

* фильтрация пакетов и контроль доступа. pfSense предоставляет возможность создавать сложные правила фильтрации пакетов и контроля доступа. Это позволяет администраторам настраивать различные политики безопасности для разных сегментов сети;
* защита от внешних угроз. Встроенные функции IDS/IPS (системы обнаружения и предотвращения вторжений) в pfSense позволяют эффективно защищать сеть от множества угроз, таких как атаки на веб-серверы, DDoS-атаки и другие виды вредоносной активности;
* поддержка VPN. pfSense поддерживает создание различных типов VPN (IPsec, OpenVPN, PPTP), что позволяет безопасно подключать удаленных сотрудников и филиалы компании;
* мониторинг и управление. pfSense предоставляет обширные возможности для мониторинга трафика и управления сетью. Интуитивно понятный веб-интерфейс позволяет удобно управлять устройством, настраивать правила и отслеживать события безопасности;
* сегментация сети. Возможность создания VLAN (виртуальных локальных сетей) помогает сегментировать сеть на несколько изолированных подсетей;
* обновления и поддержка. pfSense регулярно получает обновления, которые включают исправления безопасности и новые функции. Активное сообщество и коммерческая поддержка от компании Netgate обеспечивают оперативное решение возникающих проблем и постоянное улучшение продукта.

pfSense предлагает значительные преимущества для "Калуга-Стройдом":

* экономичность. pfSense является бесплатным и открытым программным обеспечением, что значительно сокращает затраты на обеспечение сетевой безопасности по сравнению с коммерческими решениями;
* гибкость и масштабируемость. pfSense можно развернуть на различных аппаратных платформах, начиная от маломощных устройств до мощных серверов;
* богатый набор функций. Широкий спектр возможностей pfSense, таких как поддержка VPN, IDS/IPS, фильтрация URL и контента, делает его универсальным инструментом для обеспечения безопасности сети;
* простота управления. Интуитивно понятный веб-интерфейс и богатая документация делают pfSense удобным в управлении даже для администраторов с базовыми знаниями сетевой безопасности;
* коммерческая поддержка. В случае необходимости можно воспользоваться платными услугами компании Netgate, что обеспечивает дополнительную уверенность в надежности и безопасности сети.

В заключение, pfSense представляет собой мощный и гибкий программный межсетевой экран, который идеально подходит для защиты сети строительной компании "Калуга-Стройдом". Его использование поможет обеспечить надежную защиту данных, снизить риски утечек информации и повысить общую безопасность ИТ-инфраструктуры компании.

Программное обеспечение для безопасной печати играет ключевую роль в обеспечении безопасности конфиденциальной информации и эффективности процессов печати в организациях. Оно предоставляет комплексные решения для контроля доступа к принтерам и управления печатными заданиями, минимизируя риски утечки данных и несанкционированного доступа.

Основной задачей такого программного обеспечения является обеспечение безопасности всего процесса печати, начиная с аутентификации пользователей и заканчивая защитой передаваемых данных. Аутентификация пользователей может осуществляться различными способами, такими как ввод пароля, использование биометрических данных или специальных карт доступа.

Управление правами доступа к принтерам и печатным функциям также является важной функцией программного обеспечения для безопасной печати. Оно позволяет настраивать права доступа для различных групп пользователей и ограничивать использование определенных функций печати в зависимости от роли сотрудника или его группы.

Программное обеспечение для безопасной печати предоставляет целый ряд преимуществ, включая защиту конфиденциальной информации, повышение отчетности и контроля над процессом печати, а также снижение затрат на использование принтеров и расходных материалов. Эффективное использование такого программного обеспечения помогает организациям обеспечить безопасность и эффективность процессов печати, что является ключевым аспектом информационной безопасности в современном бизнесе.

Papercut — это программное обеспечение для управления печатью, которое обеспечивает централизованный контроль и управление процессами печати в организации. Оно предоставляет широкий спектр функций, позволяющих управлять распечаткой, контролировать расходы на печать и обеспечивать безопасность печатных заданий (рисунок 30).

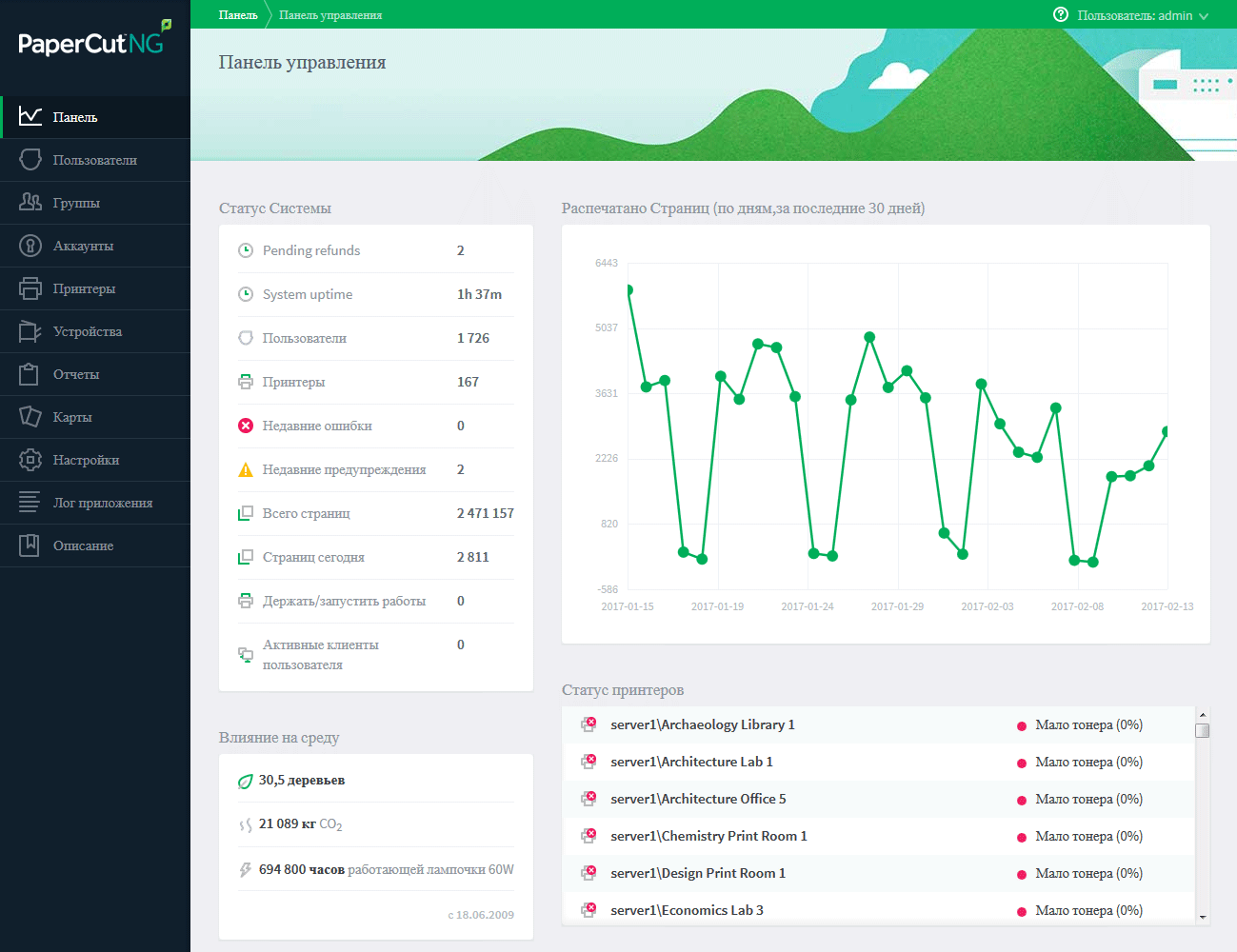


Рисунок 30 - PaperCut

Основные возможности Papercut включают:

* управление печатью. Papercut позволяет управлять всеми аспектами печати в сети, включая управление принтерами, очередями печати, настройку параметров печати и др;
* контроль расходов. Программное обеспечение позволяет отслеживать и контролировать расходы на печать, включая учет расходных материалов и определение стоимости печати для каждого пользователя или группы пользователей;
* безопасность печати. Papercut обеспечивает защиту конфиденциальной информации и предотвращает несанкционированный доступ к печатным заданиям путем внедрения механизмов аутентификации пользователей и шифрования данных;
* отчетность и аналитика. Программное обеспечение предоставляет возможности для мониторинга и анализа использования принтеров, а также генерации отчетов о печатных заданиях, расходах на печать и др;
* гибкость и настраиваемость. Papercut позволяет настраивать параметры печати в соответствии с потребностями организации и предоставляет гибкие инструменты для адаптации к различным бизнес-процессам.

Использование Papercut помогает организациям управлять и оптимизировать процессы печати, повышать эффективность использования принтеров и снижать расходы на печать, что делает его популярным выбором для организаций любого размера и направления.

В заключении можно подчеркнуть важность правильного выбора и настройки таких средств для обеспечения надежной защиты информации. Ограничение доступа к программам и данным является ключевым аспектом информационной безопасности, поскольку позволяет предотвращать несанкционированный доступ к конфиденциальным данным и снижать риск утечек информации.

Оптимальный выбор средств ограничения программной среды должен учитывать специфику деятельности компании, особенности используемых программ и данных, а также требования к безопасности. При этом необходимо обеспечить удобство использования для авторизованных пользователей и минимизировать издержки на администрирование и поддержку системы.

# **ГЛАВА 3. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАБОТ**

# 3.1. Расчет затрат на оборудование

Для организации бизнес-процессов современных предприятий в настоящее время информационные технологии приобретают всё более важное значение. Информационные технологии становятся главным фактором экономического роста информационные технологии — это совокупность методов, производственных процессов и программно-технических средств, объединены в технологическую цепочку, обеспечивающую сбор, обработку, вывод и распространение информации.

Информационные технологии включают технические и программные средства для хранения, обмена и распространения информации.

Современные достижения в развитии информационных технологий привели к формированию глобальной электронной среды для экономической деятельности, что открыло новые возможности в области организации бизнеса. Электронная среда для экономической деятельности приобрела название «Сетевая экономика».

1. **Краткое описание предметной области и области ее применения**

Компания "Калуга-Стройдом" создала Комплексную Систему Защиты Информации (КСЗИ) для защиты конфиденциальности данных проектов, технических решений и персональных данных. Это улучшит защиту от утечек информации и кибератак, обеспечивая соблюдение законодательства и повышение доверия клиентов.

1. **Расчёт себестоимости комплексной системы защиты информации**

В таблице №18, приведённой ниже, представлена калькуляция статей издержек для фирм (предприятий), специализирующихся на разработке и создании комплексных систем защиты информации.

Таблица 19. Расчёт себестоимости комплексной системы защиты информации

|  |  |  |
| --- | --- | --- |
| **№ статьи** | **Наименование статьи** | **Сумма (руб.)** |
| 1 | Материалы | 1852185 |
| 2 | Расходы на оплату труда | 835000 |
| 3 | Страховые взносы | 250500 |
| 4 | Амортизация | 2639 |

Продолжение таблицы 19. Расчёт себестоимости комплексной системы защиты информации

|  |  |  |
| --- | --- | --- |
| 5 | Расходы на содержание зданий, инвентаря, АУП и прочие накладные расходы (данные расходы составляют 50-80 % от суммы расходов на оплату труда) | 584500 |
| 6 | Всего издержек | 3524824 |

**Страховые взносы с ФОТ**

Страховые взносы составляют 30 % с фонда оплаты труда.

**835000** *\*30%/100% = (250500) в рублях.*

Амортизация основных средств

а) амортизация компьютера

месячная норма амортизации: **А=годовая норма/12 мес.**

**1.Сумма аморт. комп. = А\*стоимость компьютера**

***Сам=Аком\*Ском/100%/12****, где*

Сам - амортизация компьютера

Аком - норма амортизации компьютера (%) - 1/срок службы (5 лет) \*100%

Ском - стоимость компьютера (руб.)

***2.Сам= 135000* *\*20%/100%/12= 2250 руб.***

б) амортизация компьютерного кабинета:

Стоимость основных фондов (стоимость здания) = (7000000) руб.

Годовая норма амортизации =2%

месячная норма амортизации: А=годовая норма/12 мес.

Сумма аморт. здания = 0,167%\*7000000 = (11690)

Сумма аморт. здания в целом = 2/100%/12\* (стоимость здания\*)

Сумма аморт. компьютерного кабинета = (Сумма аморт. здания/площадь здания) \*площадь кабинета:

***(11690/450) \*15=389 руб.***

Итого амортизационных отчислений:

Сумма амортизации компьютера + Сумма амортизации кабинета

***2250 + 389 = 2639 руб.***

Прочие издержки

Прочие издержки принимаются в объёме 50-80% от суммы з/п (Ф)

***835000\*70%/100%= 584 500 руб.***

**Всего издержек по разработке**

**РМИ+РИЗ+ЕСН+ИЭ+АОС+ИО+ПИ = *3512112 руб.***

1. Расчёт материальных издержек

Таблица 20. Расчет материальных издержек

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Кол-во** | **Стоимость (руб.)** | **Сумма (руб.)** |
| 1 | Электронный замок Private Vescona | 9 | 16074 | 144666 |
| 2 | Карта доступа Em-marine | 36 | 155 | 5580 |
| 3 | Шлагбаум CAME Gard 4000 | 1 | 57222 | 57222 |
| 4 | Калитка распашная с панелью | 1 | 28940 | 28940 |
| 5 | Турникет "Ростов-Дон Т9М1-02" | 1 | 82844 | 82844 |
| 6 | Видеокамера TP-Link Tapo C500 | 18 | 3299 | 59382 |
| 7 | IP камера Hikvision 1.68мм (DS-2CD2345G0P-I) | 2 | 19450 | 38900 |
| 8 | Термошкаф уличный навесной МАСТЕР-3 УТ | 2 | 12412 | 24824 |
| 9 | Коммутатор TP-LINK TL-SG1005LP | 10 | 1590 | 15900 |
| 10 | Кабель Ethernet для IP камеры видеонаблюдения Onviz | 5 | 960 | 4800 |
| 11 | PoE коммутатор IPTRONIC PS2-E28P24M | 1 | 31146 | 31146 |
| 12 | ИБП APC Back-UPS 650VA 230V AVR Schuko | 1 | 4560 | 4560 |
| 13 | Сервер Dell R630 8SFF | 1 | 54351 | 54351 |
| 14 | Огнетушитель ОП-4(з)-АВСЕ-01 | 5 | 618 | 3090 |
| 15 | Извещатель пожарный дымовой автономный  ИП 212-50М2 | 16 | 991 | 15856 |
| 16 | Извещатель пожарный ручной адресный Болид ИПР 513-3АМ | 6 | 1161 | 6966 |
| 17 | КПУ11-16/11 (реверс) TDM | 1 | 1541 | 1541 |
| 18 | DS-PDPG12P-EG2-WE PIR датчик беспроводной с детекцией разбития стекла | 9 | 7830 | 70470 |
| 19 | ИК датчик движения потолочный | 14 | 618 | 8652 |
| 20 | Wi-Fi роутер MikroTik RB4011iGS+5HacQ2HnD-IN | 1 | 37799 | 37799 |
|  | **Итого:** |  |  | **697489** |

1. Расчёт издержек на зарплату

Таблица 21. Расчет издержек на зарплату

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Категория персонала** | **Оклад (руб.)** | **Зарплата за 160 часов** | **Премия от з/п (30%)** | **Итого (руб.)** |
| Директор | 84000 | 120000 | 36000 | 120000 |
| Архитекторы | 56000 | 80000 | 24000 | 80000 |
| Инженеры | 49000 | 70000 | 21000 | 70000 |
| Дизайнеры | 45500 | 65000 | 19500 | 65000 |
| Прорабы | 42000 | 60000 | 18000 | 60000 |
| Мастера | 38500 | 55000 | 16500 | 55000 |
| Бригадиры | 35000 | 50000 | 15000 | 50000 |
| Менеджеры | 31500 | 45000 | 13500 | 45000 |
| Операционисты | 28000 | 40000 | 12000 | 40000 |
| Начальник склада | 35000 | 50000 | 15000 | 50000 |
| Бухгалтеры | 38500 | 55000 | 16500 | 55000 |
| Агенты поддержки | 28000 | 40000 | 12000 | 40000 |
| Сис. Админы | 42000 | 60000 | 18000 | 60000 |
| Специалист отдела кадров | 31500 | 45000 | 13500 | 45000 |
| **Всего зарплата:** |  |  |  | **835000** |

# 3.2. Расчет затрат на программное обеспечение

Таблица 22. Расчет затрат на ПО

|  |  |  |  |
| --- | --- | --- | --- |
| ПО | Кол-во | Стоимость (руб) | Сумма (руб) |
| Active Directory | 1 | 89575 | 89575 |
| Kaspersky endpoint security | 19 | 52620 | 999780 |
| PaperCut | 1 | 103140 | 103140 |

# 3.3. Оценка экономической эффективности работы

Оценка экономической эффективности работы – это важный этап анализа и планирования, который позволяет определить, насколько результативной является деятельность компании или отдельного проекта. Экономическая эффективность может быть измерена различными методами и показателями, такими как рентабельность, окупаемость инвестиций, экономия затрат и повышение производительности.

Для начала необходимо четко определить цели, которые ставятся перед оценкой экономической эффективности. Это может быть увеличение прибыли, снижение затрат, улучшение качества продукции или услуг, увеличение рыночной доли и т.д. Критерии оценки должны быть конкретными, измеримыми, достижимыми, релевантными и ограниченными во времени.

Следующий шаг – сбор данных, необходимых для оценки. Это включает информацию о затратах на производство, эксплуатацию и обслуживание, доходах от продаж, объемах продаж, изменениях в производительности и других показателях, которые влияют на экономическую эффективность.

Для оценки экономической эффективности используются различные финансовые и экономические показатели.

Рентабельность (ROI) – отношение чистой прибыли к общим инвестициям.

Период окупаемости (Payback Period) – время, необходимое для возврата первоначальных инвестиций.

Экономия затрат – разница между затратами до и после внедрения улучшений. Экономия затрат позволяет оценить, насколько внедрение новых технологий или оптимизация процессов сократили расходы.

Производительность труда – отношение объема выполненных работ к затраченному времени.

После расчета показателей необходимо проанализировать результаты. Сравнение текущих показателей с предыдущими периодами или с аналогичными компаниями позволяет выявить сильные и слабые стороны. На основе анализа принимаются решения о дальнейших действиях: продолжении текущих стратегий, внедрении новых технологий, оптимизации процессов и т.д.

Эффективность работы должна постоянно контролироваться и оцениваться. Регулярный мониторинг позволяет своевременно выявлять отклонения от плановых показателей и принимать корректирующие меры. Постоянный контроль и оценка эффективности способствуют устойчивому развитию компании и достижению поставленных целей.

Тщательный анализ и правильное применение методов оценки позволяют повысить производительность, снизить затраты и улучшить финансовые результаты. Это, в свою очередь, способствует устойчивому развитию бизнеса и повышению его конкурентоспособности на рынке.

# **ЗАКЛЮЧЕНИЕ**

В рамках данной дипломной работы была проведена комплексная оценка текущего состояния информационной среды строительной компании, разработаны рекомендации по совершенствованию системы защиты информации и предложены методы повышения экономической эффективности работы предприятия. В ходе анализа было выявлено, что информационная среда компании включает разнообразные технические и программные средства, обеспечивающие выполнение ключевых бизнес-процессов. Были описаны основные элементы инфраструктуры, такие как серверы, рабочие станции, сетевое оборудование и специализированное программное обеспечение для проектирования и управления строительными проектами.

Были рассмотрены различные средства защиты информации, включая антивирусное ПО, межсетевые экраны, системы аутентификации и авторизации. Особое внимание уделено практическому применению решений, таких как Active Directory для управления пользователями и доступом, и антивирусное ПО Kaspersky для обеспечения безопасности рабочих станций и серверов. Проведен подробный расчет себестоимости создания комплексной системы защиты информации (КСЗИ), включающий затраты на материалы, оплату труда, страховые взносы, амортизацию основных средств и прочие расходы. Оценена экономическая эффективность внедрения КСЗИ, определены основные финансовые показатели.

Создание и внедрение КСЗИ позволит значительно повысить уровень защищенности информации в строительной компании, минимизировать риски утечек данных и несанкционированного доступа. Оптимизация информационной среды и внедрение современных технологий управления информацией способствуют повышению производительности труда и снижению эксплуатационных затрат. Экономическая оценка показала, что инвестиции в систему защиты информации окупаются за счет сокращения расходов на устранение последствий инцидентов безопасности и повышения эффективности работы компании.

Для дальнейшего углубления темы и улучшения системы защиты информации в строительной компании можно рассмотреть следующие направления:

* внедрение более продвинутых технологий и методов защиты, таких как искусственный интеллект и машинное обучение для проактивного обнаружения угроз;
* проведение регулярных аудитов безопасности и тестов на проникновение для оценки эффективности текущих мер защиты и выявления возможных уязвимостей;
* разработка и внедрение программ обучения и повышения осведомленности сотрудников в области информационной безопасности, чтобы минимизировать человеческий фактор как одну из основных угроз.

Конкретные задачи для будущих исследователей включают исследование новых технологий и решений в области информационной безопасности, которые могут быть применены в строительной отрасли, разработку методик оценки эффективности различных мер защиты и их адаптацию к специфике деятельности строительных компаний, анализ и систематизацию опыта других компаний в области создания и эксплуатации КСЗИ для разработки лучших практик и рекомендаций.

Проведенная работа и полученные результаты представляют значительный вклад в улучшение информационной безопасности и экономической эффективности строительной компании. Внедрение предложенных рекомендаций позволит компании не только повысить уровень защиты информации, но и укрепить свои позиции на рынке, благодаря более эффективному управлению ресурсами и процессами.

# **БИБЛИОГРАФИЯ**

Нормативные правовые акты

1. Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ.
2. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года.
3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных".
5. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".

Научная литература и материалы периодической печати

1. Бейли, Дж. и другие. "Управление IT-инфраструктурой и IT-сервисами". Издательство "Бином", 2021.
2. Блох, Дж. "Эффективное программирование: Введение в искусство разработки ПО". Издательство "Питер", 2021.
3. Вайнбергер, Д. "Информационная архитектура: как управлять информацией в компании". Издательство "Манн, Иванов и Фербер", 2020.
4. Гусев, А. В. "Информационная безопасность: Теория и практика". Издательство "Эксмо", 2019.
5. Иванов, А. А. "Комплексные системы защиты информации". Издательство "Юрайт", 2021.
6. Кейн, Дж. "Информационные технологии и управление". Издательство "Вильямс", 2019.
7. Козлов, В. Н. "Технические средства защиты информации". Издательство "МГТУ им. Баумана", 2020.
8. Лившиц, Б. "Программное обеспечение: Разработка и защита". Издательство "Бином", 2019.
9. Мур, С. "Безопасность информационных систем". Издательство "Питер", 2019.
10. Романов, А. В. "Информационная безопасность в современных организациях". Издательство "Юрайт", 2019.
11. Сидоров, И. В. "Основы информационной безопасности". Издательство "Альпина Паблишер", 2020.
12. Тихомиров, Н. А. "Методы и средства защиты информации". Издательство "Лань", 2021.
13. Фишер, Т. "Управление данными: Руководство для профессионалов". Издательство "Питер", 2020.
14. Чернов, И. С. "Современные технологии защиты информации". Издательство "Высшая школа", 2021.
15. Шнайдер, Б. "Компьютерная безопасность: Принципы и практика". Издательство "Питер", 2022.

Ресурсы Интернет

1. Cisco Systems. Руководства и документы по безопасности. URL: https://www.cisco.com/c/en/us/products/security/index.html.
2. Gartner. Исследования по информационной безопасности. URL: https://www.gartner.com/en/information-technology/security.
3. IBM Security. URL: https://www.ibm.com/security.
4. InfoWatch. Решения по информационной безопасности. URL: https://infowatch.ru.
5. IT-книга. Информационные технологии и безопасность. URL: https://itbook.ru.
6. Kaspersky Lab. Официальный сайт. URL: https://www.kaspersky.ru.
7. Microsoft Active Directory. URL: https://docs.microsoft.com/ru-ru/windows-server/identity/active-directory-domain-services.
8. Oracle Security. Документы и рекомендации. URL: https://www.oracle.com/security.
9. Symantec (Norton). Советы и инструменты по защите данных. URL: https://www.symantec.com.
10. TechRepublic. Руководства по кибербезопасности. URL: https://www.techrepublic.com.
11. Государственная система обеспечения информационной безопасности Российской Федерации (ГСОИБ). URL: http://www.gosobzor.ru.
12. Комплексные решения по защите данных от Positive Technologies. URL: https://www.ptsecurity.com/ru-ru.
13. Лаборатория Касперского. Блоги и аналитика. URL: https://www.securelist.ru.
14. Сайт по безопасности данных Habrahabr. URL: https://habr.com/ru/hub/infosecurity.
15. Советы по информационной безопасности от Microsoft. URL: https://www.microsoft.com/ru-ru/security.
16. Форум по информационной безопасности RusCrypto. URL: https://www.ruscrypto.ru.
17. Форум по информационной безопасности SecurityLab. URL: https://www.securitylab.ru.
18. ФСТЭК России. Официальный сайт. URL: https://fstec.ru.