**СОДЕРЖАНИЕ**

[Введение 6](#_Toc168941212)

[1 Проведение предпроектного обследования организации 8](#_Toc168941213)

[1.1 Выявление защищаемой информации и описание информационной…... системы 8](#_Toc168941214)

[1.2 Описание технологического процесса обработки информации………... выявление объектов защиты 11](#_Toc168941216)

[1.3 Определение угроз и уязвимостей выявленных объектов защиты………. информации. 18](#_Toc168941217)

[2 Проектирование системы защиты информации 20](#_Toc168941218)

[2.1 Определение мер защиты информации для организации 20](#_Toc168941219)

[2.2 Определение средств защиты информации 21](#_Toc168941220)

[3 Реализация средств защиты информации 30](#_Toc168941221)

[3.1 Модернизация программно-технической системы защиты информации.. 30](#_Toc168941222)

[3.2 Оценка системы защиты информации 35](#_Toc168941223)

[3.3 Экономическое обоснование 42](#_Toc168941224)

[Заключение 44](#_Toc168941225)

[Список использованных источников 46](#_Toc168941226)

**ОПРЕДЕЛЕНИЯ**

Несанкционированный доступ — доступ к информации, осуществляемый с нарушением установленных правил

Система защиты информации — совокупность организационных, правовых, технических и иных мер, направленных на обеспечение сохранности информации от несанкционированного доступа, изменения, уничтожения или раскрытия

Система контроля и управления доступом — система, предназначенная для управления доступом к объектам, в которой производится идентификация лиц, имеющих право доступа, и проверка соответствия их прав доступу к объекту.

Информационная безопасность — состояние, при котором уровень риска для информационных активов приемлем.

Программное обеспечение — совокупность программ, процедур, документации, относящихся к работе ЭВМ и позволяющих выполнять определенные задачи.

Автоматизированное рабочее место — комплекс средств вычислительной техники, программного обеспечения и документации, предназначенный для выполнения задач пользователем

[Контролируемая зона — это территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств без постоянного или разового допуска](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%B8%D1%80%D1%83%D0%B5%D0%BC%D0%B0%D1%8F_%D0%B7%D0%BE%D0%BD%D0%B0)

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

СЗИ — системы защиты информации.

НСД — несанкционированный доступ.

ТМЗИ — технических меры защиты информации.

ПМЗИ —программные меры защиты информации.

ПО — программное обеспечение.

ИБ — информационная безопасность.

АРМ — автоматизированное рабочее место.

ИС — информационная система.

# **ВВЕДЕНИЕ**

В современном мире, где информация стала одним из ключевых ресурсов, вопросы её защиты приобретают особую актуальность. Это особенно важно для предприятий, занимающихся производством и обработкой товаров, таких как ООО «Картонтара» (далее «Картонтара»). Защита информации на таких объектах требует разработки и внедрения эффективных программно-технических мероприятий.

Целью данного дипломного проекта является разработка программно-технических мероприятий по защите информации на объекте ООО «Картонтара».

В рамках достижения данной цели ставятся следующие задачи:

* выявить защищаемую информацию;
* определить угрозы и уязвимости;
* определить меры защиты информации;
* определить средства защиты информацтт;
* проектирование системы защиты информации.

На сегодняшний день существует множество СЗИ, однако, не все из них способны обеспечить адекватный уровень защиты в условиях специфики работы объекта ООО «Картонтара». Важным аспектом данного исследования является выявление этих недостатков и предложение нового подхода к созданию более эффективной СЗИ.

Объектом исследования являются СЗИ в «Картонтара».

Предметом исследования являются существующие программно-технические мероприятия по защите информации. Разработка эффективной СЗИ будет проведена на основе анализа научных статей, литературы и существующих систем.

Методы исследования включают в себя теоретический анализ принципов защиты информации, сравнительный анализ существующих систем, а также практическую оценку СЗИ для оценки эффективности разработанной системы. Важным этапом работы будет также анализ законодательной базы в области защиты информации, что позволит учесть все нормативные требования при разработке СЗИ. Кроме того, будет проведена работа по обучению персонала основам безопасности информации и правилам работы с новой системой, что повысит эффективность её использования и снизит риск случайных утечек информации.

# **1 ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ ОРГАНИЗАЦИИ**

Данная глава посвящена анализу организации «Картонтара». Изучению бизнес-процессов и анализ текущей СЗИ. Целью данного анализа является определения уязвимостей и недостатков СЗИ.

1.1 Выявление защищаемой информации и описание информационной системы

Организация «Картонтара»– это ведущий производитель гофроупаковки и макулатурного картона в России.

«Картонтара», расположенное в Адыгее, осуществляет обработку и сохранение базовых данных. В структуре компании можно выделить несколько ключевых отделов:

* отдел производства;
* отдел продаж;
* отдел закупок;
* отдел финансов;
* отдел маркетинга и PR;
* отдел управления персоналом;
* отдел информационных технологий.

Отдел производства отвечает за разработку, проектирование и изготовление продукции компании. Отдел продаж занимается продвижением и продажей продукции. Отдел закупок отвечает за закупку сырья и материалов для производства. Отдел логистики отвечает за доставку продукции до конечного потребителя. Отдел финансов занимается финансовым планированием, бюджетированием и учетом. Отдел маркетинга и PR отвечает за создание и реализацию маркетинговых стратегий. Отдел информационных технологий отвечает за поддержание и обновление всей информационной инфраструктуры компании. Отдел управления персоналом занимается всеми вопросами, связанными с наймом, обучением, развитием и увольнением сотрудников. Он также отвечает за вопросы трудового законодательства.

Для выполнения своих функциональных обязанностей, все отделы в организации «Картонтара» обрабатывают персональные данные сотрудников и коммерческую тайну:

* основная информация: ФИО, дата рождения, гражданство, пол, место рождения;
* контактная информация: Адрес проживания, номер телефона, адрес электронной почты;
* информация о трудовой деятельности: Должность, отдел, дата начала работы, трудовой стаж, информация о профессиональных навыках и квалификации;
* информация о зарплате: Размер зарплаты, банковские реквизиты для выплаты зарплаты;
* информация о социальном и пенсионном страховании: Номер страхового свидетельства обязательного пенсионного страхования (СНИЛС), номер полиса обязательного медицинского страхования (ОМС).

В соответствии с категорией обрабатываемых данных, объемом, типами угроз и категорией субъектов персональных данных, для организации был установлен 4-й уровень защиты. [Это решение основывается на требованиях, установленных Постановлением Правительства РФ от 01.11.2012 N 11191](https://base.garant.ru/70252506/).

[Данное Постановление устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных1](https://base.garant.ru/70252506/). [Безопасность персональных данных обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы1](https://base.garant.ru/70252506/). [Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах1](https://base.garant.ru/70252506/).

Таким образом, выбор 4-го уровня защиты обоснован требованиями Постановления Правительства РФ от 01.11.2012 N 1119 и спецификой обрабатываемых в организации данных. Данные сведения, в соответствии указом Президента 188, является конфиденциальными в следствии защита этих данных обязательна в соответствии с законодательством, в частности, с Федеральным законом «О персональных данных» № 152-ФЗ

### **1.1.1 Анализ нормативных документов.**

Положения о внутреннем контроле. Этот документ описывает процедуры и меры, которые организация принимает для обеспечения соблюдения законов и нормативов.

Положения о персональных данных. Этот документ описывает, как организация обрабатывает и защищает персональные данные.

Правила внутреннего трудового распорядка. Этот документ устанавливает правила поведения для сотрудников организации.

Положения о бухгалтерском учете и отчетности. Этот документ описывает процедуры и стандарты, которые организация следует при ведении бухгалтерского учета и составлении отчетности.

Положения о корпоративной безопасности. Этот документ описывает меры, которые организация принимает для обеспечения безопасности своих активов и персонала.

* защита персональных данных. Необходимо обеспечить, что персональные данные обрабатываются и хранятся в соответствии с положениями о персональных данных;
* внутренний контроль и аудит. Необходимо убедиться, что организация имеет эффективные системы внутреннего контроля и аудита для обеспечения соблюдения всех применимых законов и нормативов;
* соблюдение правил внутреннего трудового распорядка. Необходимо обеспечить, что все сотрудники знают и соблюдают установленные правила поведения;
* бухгалтерский учет и отчетность. Необходимо убедиться, что организация следует установленным процедурам и стандартам при ведении бухгалтерского учета и составлении отчетности;
* корпоративная безопасность. Необходимо обеспечить, что организация принимает необходимые меры для защиты своих активов и персонала.

Эти меры защиты информации помогут организации защитить свои активы, соблюсти законодательство, предотвратить утечку информации и улучшить общую безопасность. Они также помогут организации поддерживать доверие и репутацию среди своих клиентов, партнеров и общественности.

1.2 Описание технологического процесса обработки информации. Выявление объектов защиты

Все эти отделы расположены в «Здании 6». (рисунок 1).

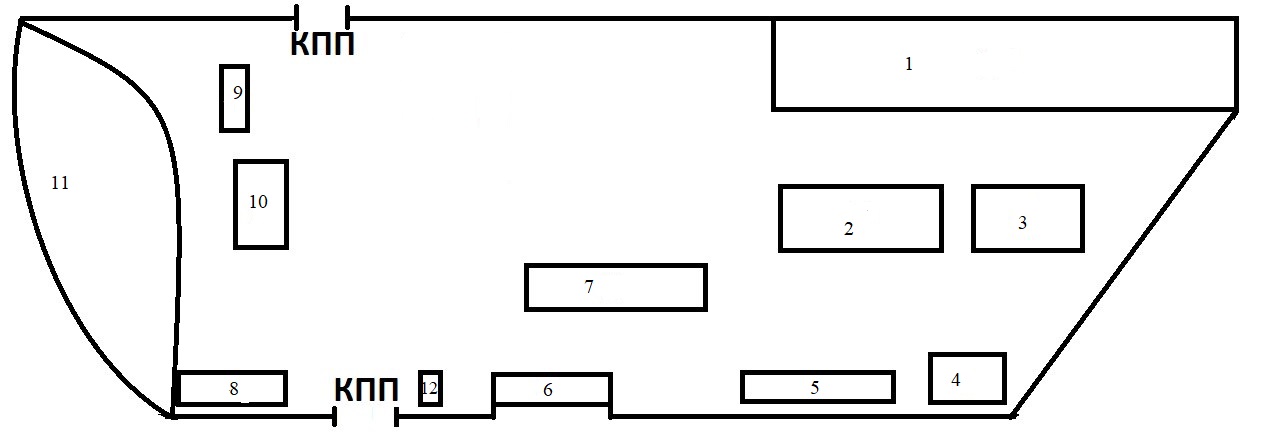


Рисунок 1 - План территории «Картонтары».

«Здание 6» является главным зданием, сюда поступает информация, со всех компьютеров, которые расположены в других зданиях.

«Здание 1» является огромным заводом, внутри производится из нужного сырья конечный материал, и там же он складируется.

«Здания 2, 3, 4, 7, 10» являются «точками» где из материалов производится сырье для того чтобы сделать конечный материал (картон).

«Здание 8» является складом, для старого оборудования.

«Здание 5» является складом для сырья.

«Картонтара» функционирует на 90 автоматизированных рабочих местах, классифицируемых на 2 типовых сегмента программно-аппаратные характеристики которых представлены в таблице 1.

Таблица 1 - Перечень и характеристика Автоматизированных рабочих мест (далее АРМ).

|  |  |  |  |
| --- | --- | --- | --- |
| № | | Аппаратные средства информации | Программные средства |
| 1 | | 2 | 3 |
| АРМ (охрана) | | Монитор: Acer K202HQLAb  Системный блок:   * TREIDCOMPUTER * Intel Core i5 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III. * поддержка 1 устройства M.2 SATA\PCI-E. | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР |
| АРМ (бухгалтерия) | | Монитор:Acer K202HQLAb  Системный блок:   * Platinum PC * Intel core i5- 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III. * поддержка 1 устройства M.2 SATA\PCI-E; | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР * 1с * AVAST |
|  | |  |  |
| Продолжение Таблицы 1 | | | |
| 1 | 2 | | 3 |
| АРМ (pr отдел) | | Монитор: Acer K202HQLAb  Системный блок:   * TREIDCOMPUTER * Intel Core i5 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III. * поддержка 1 устройства M.2 SATA\PCI-E. | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР * AVAST |
| АРМ (финансовый отдел) | | Монитор: Acer K202HQLAb  Системный блок:   * TREIDCOMPUTER * Intel Core i5 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III. * поддержка 1 устройства M.2 SATA\PCI-E. | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР * AVAST * 1с |
| АРМ (финансовый, исполнительный директора, главный бухгалтер) | | Монитор: Acer K202HQLAb  Системный блок:   * TREIDCOMPUTER * Intel Core i5 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III. * поддержка 1 устройства M.2 SATA\PCI-E. | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР * AVAST * 1с * CryptoPro |
| АРМ (сетевой отдел) | | Монитор: Acer K202HQLAb  Системный блок:   * TREIDCOMPUTER * Intel Core i5 3470(3.2ГГц) * до 8 ГБ DDR4 2933/2666/2400 * поддержка до 4 устройств SATA-III.   поддержка 1 устройства M.2 SATA\PCI-E. | * Windows * Microsoft Office * ЯНДЕКС БРАУЗЕР |

В компании «Картонтара» технологический процесс обработки информации проходит через несколько ключевых этапов. Начинается он со сбора данных из различных источников, включая сотрудников, клиентов и поставщиков. Затем следует этап обработки данных, на котором собранная информация преобразуется в полезную и управляемую форму. Этот процесс включает классификацию, организацию, анализ и интерпретацию данных. После обработки информация хранится в безопасном и доступном формате. Данные АРМ функционируют в локально вычислительной сети. (рисунок 2)

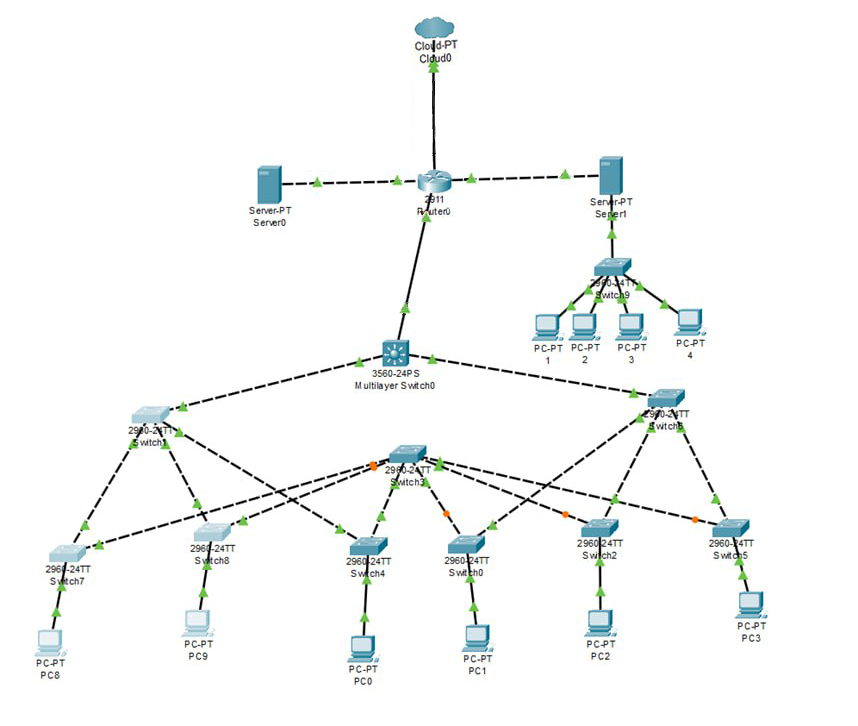


Рисунок 2 – Топология сети «Картонтары».

Все компьютеры в сети «общаются» между собой через маршрутизаторы и коммутаторы. Также на объекте используется технология VLAN. Она помогает избежать случаев НСД в информационной сфере. У каждого отдела есть собственная виртуальная сеть, которая изолирует трафик сети от других сетей. Данные рабочие места закреплены за отдельным сотрудником и имеют однопользовательский режим обработки данных. Далее будет рассмотрено «Здание 6» (рисунок 3).

Рисунок 3 – План здания №6.

На рисунке 3 изображен первый этаж плана «Здания 6», так-же изображено 3 выхода/входа. Специальным символом изображены электроно-магнитные замки. Эти замки присутствуют на лестницах и дверях переходящих в другую зону. На левом входе/выходе нет электронного замка, потому что к этому входу/выходу имеют доступ люди, которые уже прошли идентификацию (через КПП, или через другие электронные замки, которые находятся в этом здании).

Кабинет №2 является кабинетом работников кадрового отдела.

Внутри этого кабинета стоят 3 АРМ.

Кабинет №3 является кабинетом охраны.

Внутри данного кабинета стоит 1но АРМ, который также подключен к СКУД. В кабинете предусмотрено окошко, выходящее на турникет. В случае, если у посетителя отсутствует электронный пропуск для прохода через турникет, охранник запрашивает удостоверяющий личность документ. После проверки документа охранник пропускает посетителя, при необходимости открывая дверь. В случае отказа системы контроля и управления доступом (далее СКУД) - электронных замков, допуск сотрудников организации осуществляется с использованием пропуска.

Также на рисунке 3 изображен второй этаж, второй этаж нуждается в дополнительном эшелоне защиты. Ведь в кабинетах исполнительного директора, финансового директора и главного бухгалтера обрабатываются и хранятся важные данные, включая коммерческую тайну и персональные данные. Также в каждом из данных кабинетов расположены АРМ.

Также на рисунке 3 изображен третий этаж. Третий этаж, также как и второй нуждается в дополнительном эшелоне защиты. Ведь, в кабинете №37 стоят сервера, но на вход и выход в данный кабинет нет дополнительной защиты. На серверах хранятся все важные данные организации, но нет резервного хранилища.

Сервер с такими характеристиками:

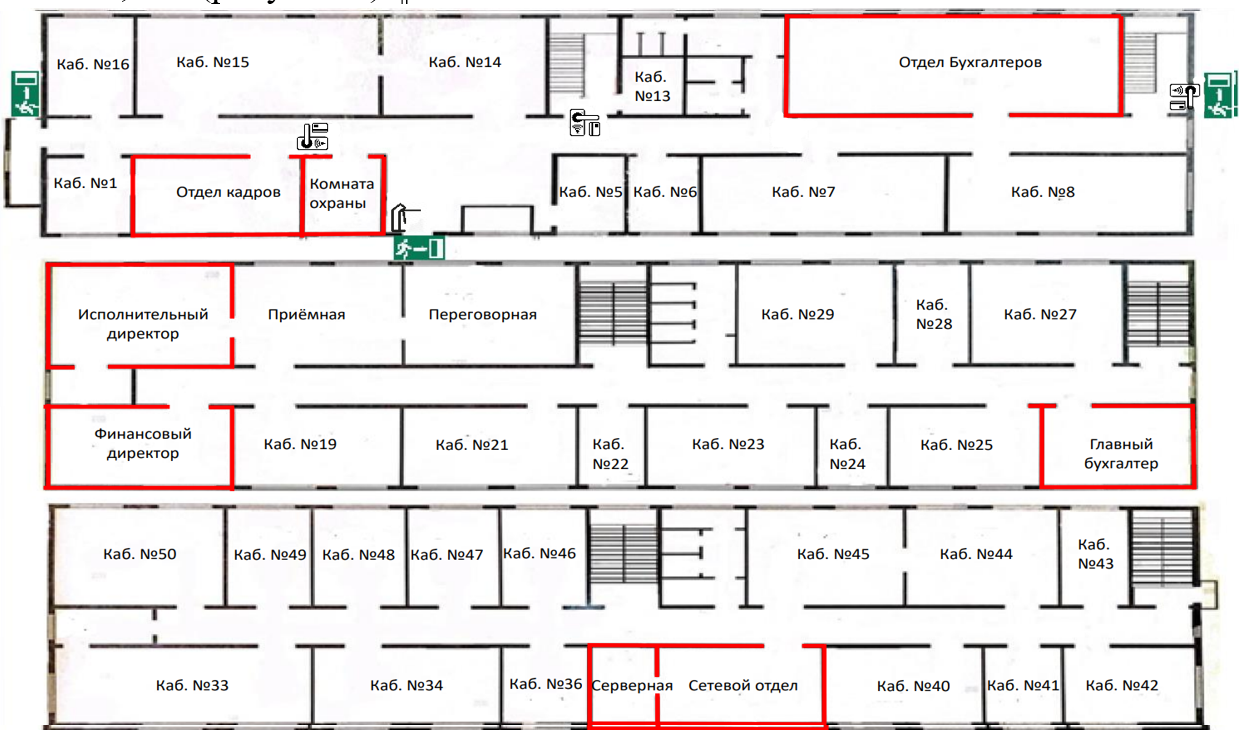
* процессоры. Масштабируемые процессоры Intel® Xeon® серии 3200-8200 и масштабируемые процессоры Intel® Xeon® серии 3100-4100.Количество ядер процессора: 4–24 ядро. Кэш процессора: 8,25–35,75 Мбайт L3;
* количество процессоров: 2;
* скорость процессора: 3,8 ГГц (максимум);
* максимальный объем памяти: 1 Тбайт при использовании модулей памяти DDR4 64 Гбайт;
* слоты памяти: 16 слотов DIMM;
* тип памяти HPE DDR4: SmartMemory;
* стандартный объем памяти: 16 ГБ (1 X 16 ГБ) RDIMM
* управление инфраструктурой: HPE iLO в стандартной комплектации с функцией Intelligent Provisioning (встроенная), HPE OneView Standard (требуется загрузка), дополнительно: HPE iLO Advanced и HPE OneView Advanced;
* блок питания: 2 блока питания HPE Flexible Slot;
* слоты расширения: 3;
* сетевой контроллер: встроенный адаптер Ethernet HPE (1 Гбит/с, 2 порта) и опциональная вертикальная плата HPE FlexibleLOM;
* контроллер памяти: контроллер HPE Smart Array S100i и 1 HPE Essential;
* функции системных вентиляторов: стандартные однороторные вентиляторы с возможностью горячей замены;
* оптический привод: DVD-ROM или DVD-RW;
* размеры продукта (В х Ш х Г): 1,69 х 17,11 х 24,21 дюйма;
* вес 15,74 кг.

В кабинете №38 стоят 4 АРМ. Данный кабинет является кабинетом системных администраторов, в котором осуществляются следующие задачи:

* системные администраторы занимаются разработкой алгоритмов для решения различных задач и их реализацией в программном коде;
* они работают над созданием надежных баз данных, обеспечивают их защиту от несанкционированного доступа и потери данных.

Исходя из всего перечисленного можно определить что контролируемая зона, это (рисунок 4):

* кабинет №2 (кабинет охраны);
* кабинет №3 (отдел кадров);
* кабинет №11(отдел бухгалтерии);
* кабинет Исполнительного директора;
* кабинет финансового директора;
* кабинет главного бухгалтера;
* кабинет №37 (сетевой отдел);
* кабинет №38 (серверная).

Рисунок 4 – контролируемая зона.

1.3 Определение угроз и уязвимостей выявленных объектов защиты информации.

Были выявлены следующие потенциальные источники угроз безопасности. Внешние источники угроз включают в себя действия хакеров или конкурентов, которые могут попытаться получить несанкционированный доступ к данным организации или совершить акты саботажа. Технические угрозы связаны с возможными недостатками в системах безопасности и отсутствием современного программного обеспечения, что может привести к появлению уязвимостей, которые могут быть использованы для несанкционированного доступа к данным. Также отсутствует система резервного копирования.

Технические утечки информации. Наличие недостатков в системе безопасности, таких как отсутствие электронных замков на входе в контролируемую зону, может позволить злоумышленникам проникнуть в эту зону без препятствий. Кроме того, отсутствие системы видеонаблюдения усиливает эту угрозу, поскольку ограничивает возможность контроля и идентификации посетителей.

# **2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

В данной главе осуществляется проектирование СЗИ. Этот процесс начинается с определения ключевых мер защиты информации, которые необходимы для обеспечения безопасности данных и информационных процессов в организации. После определения мер защиты информации, выбираются конкретные средства защиты информации. Важно отметить, что проектирование СЗИ - это не одноразовый процесс. Это непрерывная активность, которая требует регулярного пересмотра и обновления в ответ на изменяющиеся угрозы безопасности и развитие технологий. Это обеспечивает комплексный и гибкий подход к обеспечению безопасности информации в организации, позволяя адаптироваться к новым вызовам и сохранять защищенность информационных активов организации.

2.1 Определение мер защиты информации для организации

В прошлой главе был определен 4 уровень защищенности информации, отсюда следует такие меры:

* установление эффективных мер по защите от внешних угроз;
* регулярный мониторинг и аудит систем безопасности;
* ведение журналов безопасности;
* система резервного копирования;
* защита машинных носителей персональных данных;
* разграничение доступа и назначение полномочий пользователям.

[Вышеуказанные меры описаны, основываясь на федеральные законы (](https://ru.wiktionary.org/wiki/%D0%B2%D1%8B%D1%88%D0%B5%D1%83%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9)[Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»](https://base.garant.ru/12148555/). [Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»](https://base.garant.ru/12148555/). [Федеральный закон от 27 апреля 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности»](https://base.garant.ru/12148555/). [Федеральный закон от 30 марта 2011 года № 63-ФЗ «Об использовании электронной цифровой подписи»](https://base.garant.ru/12148555/). [Федеральный закон от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании»](https://base.garant.ru/12148555/)).

2.2 Определение средств защиты информации

Для установление эффективных мер по защите информации от внешних угроз, будут предложено установить электронные замки с такими требованиями:

* [высокая надежность. Электронные замки должны быть надежными и обеспечивать эффективную защиту от несанкционированного доступа](https://ilocks.ru/o-kompanii/stati-i-obzory/5233/)[;](https://bing.com/search?q=%D1%82%D1%80%D0%B5%D0%B1%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F+%D0%B4%D0%BB%D1%8F+%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D1%85+%D0%B7%D0%B0%D0%BC%D0%BA%D0%BE%D0%B2+%D0%B4%D0%BB%D1%8F+%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8)
* [оперативный монтаж и удобная эксплуатация: Замки должны быть легко устанавливаемыми и удобными в использовании](https://ilocks.ru/o-kompanii/stati-i-obzory/5233/);
* [совместимость с системами управления доступом (СКУД). Электронные замки должны быть совместимыми со СКУД и другими системами безопасности](https://ilocks.ru/o-kompanii/stati-i-obzory/5233/);
* [независимость от наличия электроэнергии. Электронные замки должны быть способны функционировать даже при отсутствии электроэнергии](https://horoshijpotolok.ru/otdelka/jelektronnyj-zamok-na-vhodnuju-dver-v-kvartiru-vidy-kak-vybrat-porjadok-ustanovki.html);
* [возможность аварийного открытия. В случае неполадок или сбоев в работе замка должна быть предусмотрена возможность аварийного открытия](https://ilocks.ru/o-kompanii/stati-i-obzory/5233/);

Такими требованиями обладает TM Touch Memory. ( рисунок 5).



Рисунок 5 – электромагнитный замок TM Touch Memory.

На рисунке 5 изображен электронный замок TM Touch Memory. С такими характеристиками:

* стандарт карт: электронные ключи-карты типа em-marine, proximity (125khz);
* элементы питания: блок-питания;
* потребление напряжения в режиме ожидания: 12мка;
* потребление напряжения в импульсном режиме: 200ма;
* закрытие замка: спустя 7 секунд после открытия замка, или сразу после нажатия ручки;
* надежность карточек: ключи-карты рассчитаны для многократной перезаписи, не менее 100000 раз. Ключи размагничиванию не подвержены;
* экстренное открывание: в экстренных ситуациях через СКУД можно открыть данные замки, также записывается, каким именно способом была открыта дверь;
* варианты врезного механизма: стандарт euro;
* размер ручки: 280мм (высота), 46мм (ширина), 20мм (толщина накладки);
* вес замка: 2,5 кг;
* интеграция с другими системами (СКУД);
* ориентация ручек: произвольная.

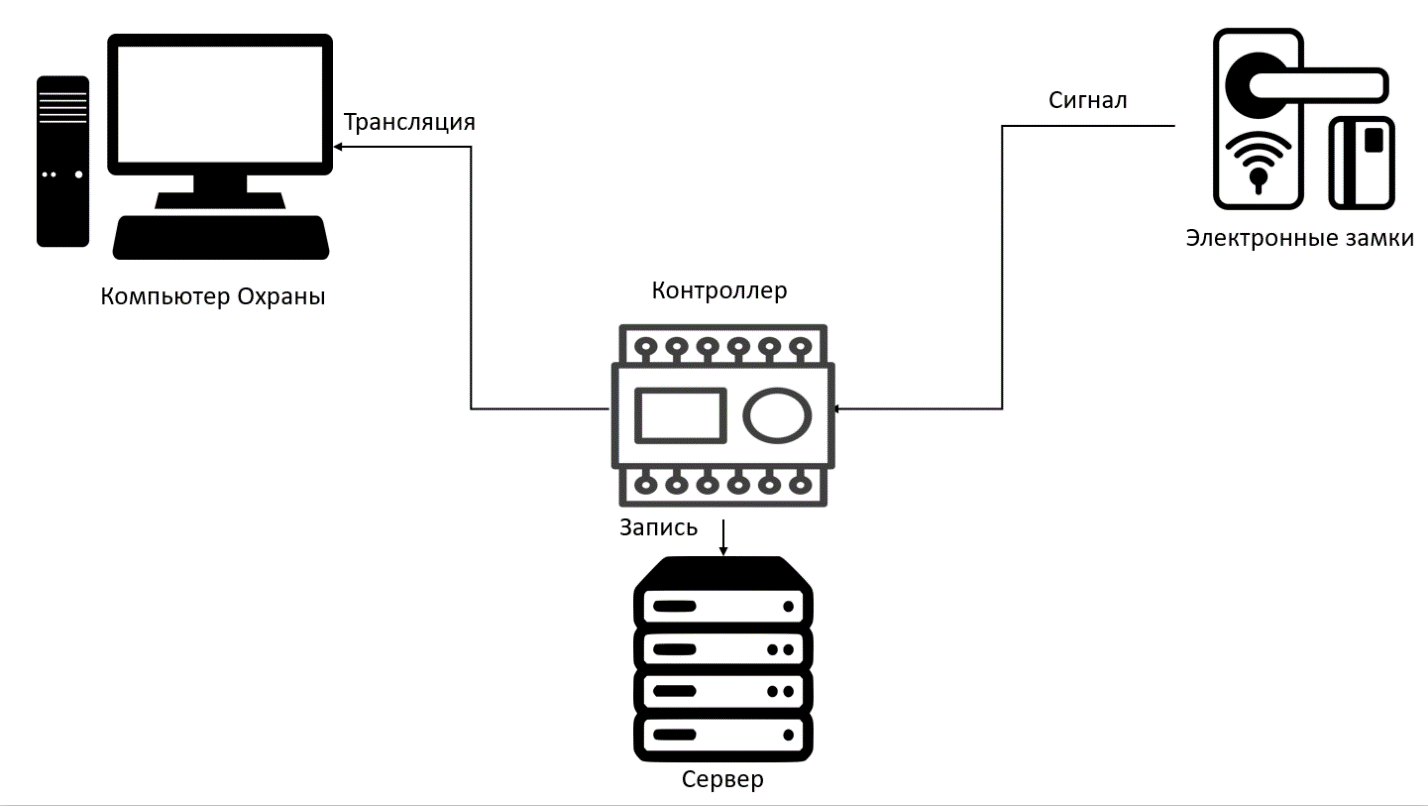
Электромагнитные замки нужно подключить к СКУД, и разграничивать права доступа электронных ключей. Чтобы каждый работник имел пропуск в свой кабинет, но не имел пропуск в чужие. СКУД теперь позволяет отслеживать время прибытия и ухода сотрудников ( рисунок 6).

Рисунок 6 – Типовая схема СКУД.

На рисунке 6 изображен принцип работы СКУД (электронные замки). При открытии двери с электронным замком идет сигнал в контроллер, который записывает на сервер и передается на компьютер охраны.

Также стоит установить видеонаблюдения с такими требованиями:

* качество видео. Система должна обеспечивать высокое разрешение видео для четкого идентификации лиц и объектов;
* покрытие. Все важные зоны, включая входы/выходы, рабочие места, склады и другие чувствительные зоны, должны быть покрыты системой видеонаблюдения;
* непрерывная запись. Система должна обеспечивать непрерывную запись 24/7 для обеспечения полного контроля;
* хранение данных. Записи должны храниться в течение определенного периода времени в соответствии с законодательством и политикой конфиденциальности компании;
* безопасность данных. Данные видеонаблюдения должны быть защищены от несанкционированного доступа. Это может включать в себя шифрование данных и использование надежных паролей;
* доступ к данным. Доступ к данным видеонаблюдения должен быть ограничен только авторизованными сотрудниками.

Такими требованиями отвечает Видеокамера Ginzzu HK-840N (см рисунок 7).

Рисунок 7 – Видеокамера Ginzzu HK-840N.

На рисунке 7 изображена камера Ginzzu HK-840N, с такими характеристиками:

* тип видеокамер: аналоговая;
* разрешение камеры: 2 мп;
* чувствительность без подсветки: 0.1 люкс;
* размер матрицы: 1/3;
* тип матрицы: sc2235;
* фокусное расстояние: 3.6 мм;
* ик подсветка: есть;
* светодиодная подсветка: есть;
* дистанция ночной съемки: 30 м.

Данные камеры продается в комплекте с видеорегистратором. С такими характеристиками:

* тип видеорегистратора: HVR(гибридный);
* форматы сжатия видео: H.264/H.264+/H.265/H.265+;
* стандарты видеосигнала: PAL/NTSC;
* количество слотов для HDD: 1;
* максимальная емкость HDD: 8тб.

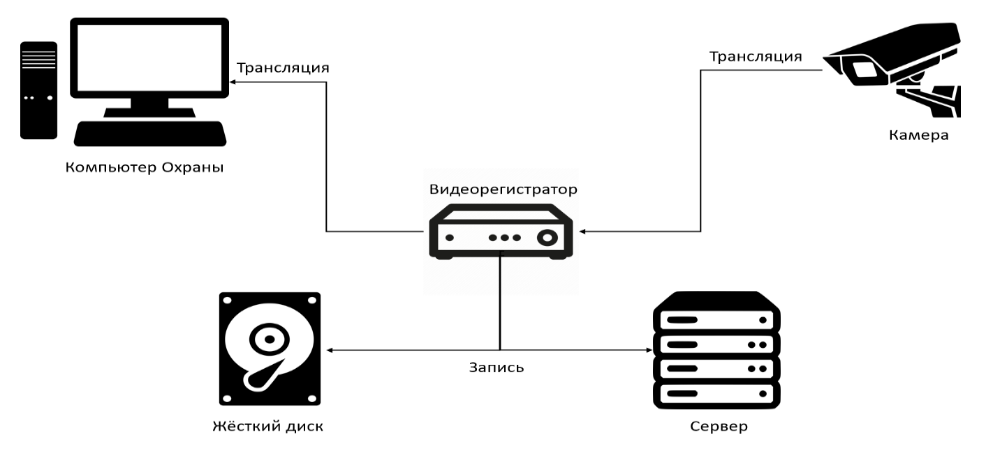
Данный видеорегистратор, нужно установить в комнату охраны, с помощью данного регистратора осуществляется мониторинг над территорией. Данные с видеокамер могут хранится как и на жестком диске, так и на удаленном сервере (рисунок 8)

Рисунок 8 – Типовая схема видеонаблюдения.

На рисунке 8 изображен принцип работы видеонаблюдения. Камера посылает сигнал в видеорегистратор, а видеорегистратор транслирует на компьютер охраны, также записывает видеозаписи на жёсткий диск и на сервер.

Secret Net Studio - это комплексное решение для обеспечения безопасности рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

Kaspersky Endpoint Security (KES) - это комплексное решение для обеспечения безопасности компьютеров от различных типов угроз, сетевых и фишинговых атак. KES предоставляет защиту в ключевых областях информационной безопасности, включая идентификацию и аутентификацию, управление доступом, защиту от вредоносного ПО, системы обнаружения вторжений, аудит и контроль, защиту информации от утечки, управление конфигурацией и изменениями

Оно обеспечивает многоуровневую защиту, включая аутентификацию пользователя, контроль целостности, замкнутую программную среду, межсетевой экран и защиту от несанкционированного доступа к конфиденциальным файлам

Ниже представлена таблица 2, которая помогает сформировать комплексное представление о различных методах защиты информации и выбрать наиболее подходящие для организации.

Таблица 2 – Программно-аппаратные меры защиты информации

|  |  |  |  |
| --- | --- | --- | --- |
| Меры ЗИ | SecretNetStudio | Kaspersky Endpoint Security | Межсетевой экран |
| 1 | 2 | 3 | 4 |
| ИАФ.1 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| УПД.1 | + | + | + |
| УПД.3 | + | + | + |
| УПД.4 | + | + | + |
| УПД.5 |  | + |  |
| |  | | --- | | Продолжение Таблицы 2 | | | | |
| 1 | 2 | 3 | 4 |
| УПД.10 | + | + | + |
| УПД.14 | + | + | + |
| УПД.15 | + | + | + |
| ОПС.2 |  | + |  |
| ОПС.3 |  | + |  |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| СОВ.2 | + | + | + |
| АРЗ.2 | + | + | + |
| АРЗ.4 | + |  |  |
| ОЦЛ.4 |  |  |  |
| ОДТ.4 |  |  |  |
| ОДТ.5 |  |  |  |
| ЗТС.3 |  |  |  |
| ЗТС.4 | + | + | + |
| ЗИС.1 | + | + | + |
| ЗИС.15 | + | + | + |
| ЗИС.20 |  |  |  |
| ИНЦ.6 | + | + | + |
| УКФ.1 |  |  |  |
| УКФ.2 | + | + | + |
| УКФ.4 | + | + | + |

Основываясь на представленной таблице, можно сделать вывод о том, что система безопасности Kaspersky Endpoint Security (KES) является оптимальным выбором для «Картонтары».

Также для повышения безопасности в сети будут далее будет предложено использовать межсетевой экран, с такими характеристиками:

* межсетевой экран должен быть сертифицирован ФСТЭК;
* межсетевой экран должен контролировать и фильтровать проходящие через него информационные потоки в соответствии с заданными правилами;
* аутентификация пользователей;
* сбор и хранение статистики событий;
* взаимодействие с другими средствами защиты информации.

Помимо это межсетевой экран должен противодействовать таким угрозам:

* нсд к цифровой информации организации;
* отказу в обслуживании информационной системы по причине неконтролируемых сетевых подключений (в том числе DDoS-атакам), уязвимостей, недостатков настроек;
* несанкционированной передаче информации из внутренней системы организации во внешнюю среду, в том числе вследствие работы вредоносного программного обеспечения;
* воздействию на межсетевой экран с целью нарушения его функционирования.

Таким требованиям отвечает межсетевой экран Континент 4 IPC-R1000 ( рисунок 9).



Рисунок 9 - Межсетевой экран Континент 4 IPC-R1000.

Он обладает такими характеристиками:

* форм-фактор: 1U;
* жесткий диск: SSD 480 ГБ;
* сетевые интерфейсы: 8x 1000BASE-T, RJ45 4x 10G SFP+;
* подключение внешнего 3G USB модема: нет;
* порт RS232 для подключения Dial-UP модема: нет;
* USB порты 2x USB 2.0, 2x USB 3.0;
* другие интерфейсы: 1x COM порт RJ45, 1x VGA для монитора (D-Sub), 1x порт с разъемом RJ12 для подключения считывателя iButton;
* блок питания: 2 х 300 Вт с функцией горячего резервирования, ~100-240 В, 3-5 А, 50-60 Гц;
* температурный режим: от 5˚С до 45˚С;
* допустимая относительная влажность: от 5% до 85%;
* допустимое атмосферное давление: от 84 до 107 кПа;
* среднее время наработки на отказ: 50 000 часов;
* габаритные размеры (мм): 500 x 430 x 44;
* вес (кг): 8,5.

# **3 РЕАЛИЗАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Для того чтобы закрыть меры, которые описаны выше, далее будут рассматриваться следующие аспекты:

* установка электромагнитных замков;
* установка видеокамер;
* установка приложений для централизованного мониторинга.

Все эти меры будут способствовать повышению уровня информационной безопасности в «Картонтара», обеспечивая защиту информационных ресурсов и бизнес-процессов от потенциальных угроз. При этом будет учтен опыт, полученный в ходе анализа текущей системы защиты информации и выявления ее уязвимостей. Это позволит «Картонтара» обеспечить надежную защиту своей информации и бизнес-процессов от любых угроз.

3.1 Модернизация программно-технической системы защиты информации.

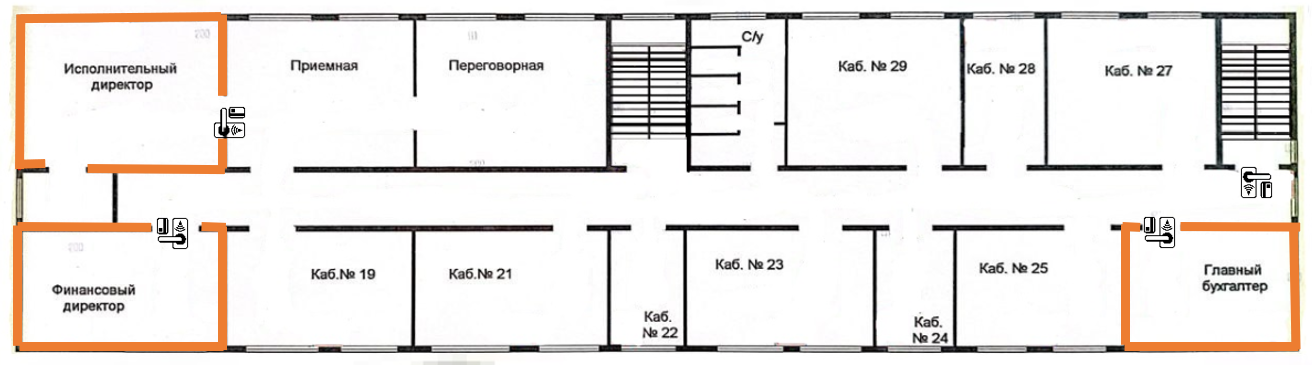
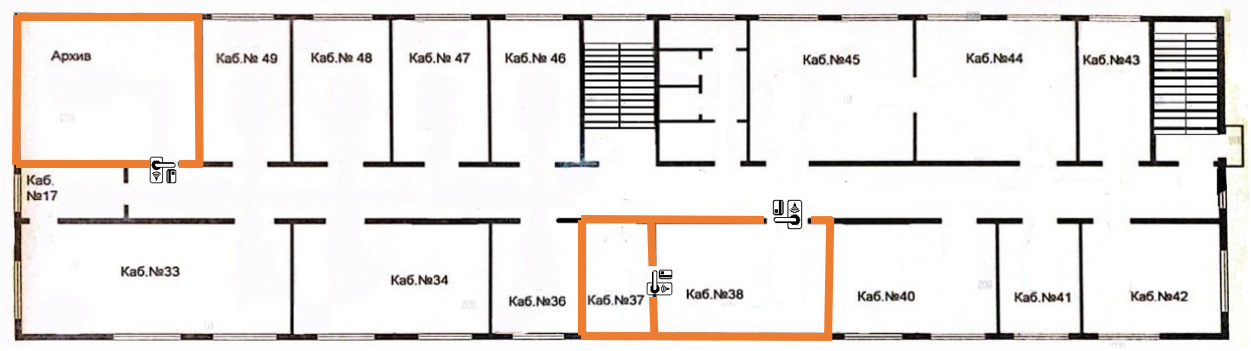
Электронные замки нужно установить на втором и третьем этажах. (рисунки 10, 11).

Рисунок 10 – Второй этаж с электронными замками.

 Рисунок 11 – Третий этаж с электронными замками.

Электронные замки стоят на вход в контролируемую зону.

Использование таких замков дает:

* электронные замки помогают предотвратить НСД и защитить данные;
* с помощью электронных замков можно точно контролировать, кто имеет доступ к определенным помещениям и в какое время;
* электронные замки могут отслеживать, кто и когда входил или выходил, что может быть полезно для аудита безопасности;
* электронные замки могут быть легко интегрированы с другими системами безопасности, такими как видеонаблюдение или системы оповещения;
* если ключи или коды доступа теряются или становятся известными, электронные замки позволяют быстро и легко изменить коды доступа или отозвать ключи.

Далее будут рассмотрены планы этажей с предлагаемыми средствами защиты информации, на рисунках 12, 13 и 14.

Рисунок 12 – Предлагаемая СЗИ первого этажа

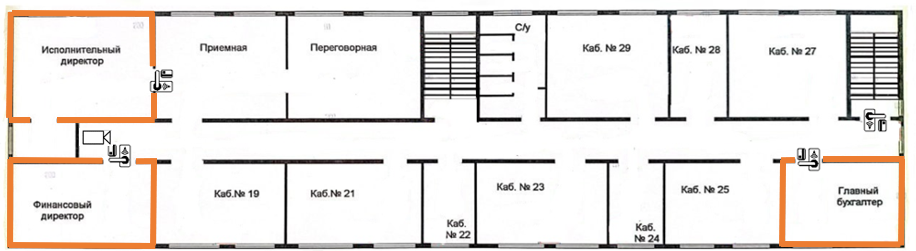
Камера с номером 1 должна видеть все входы. Камера с номером 2 должна видеть два входа с электромагнитными замками 2 входа без электромагнитных замков.

Рисунок 13 – Предлагаемая СЗИ второго этажа.

На втором этаже достаточно одной камеры, ведь на втором этаже нет дверей посреди коридоров. Но камера должна захватывать полностью коридор.

Рисунок 14 – Предлагаемая СЗИ третьего этажа этаж.

На третьем этаже также достаточно одной камеры, которая полностью просматривает коридор и все входы в кабинеты.

Использование данных средств обеспечивает ряд преимуществ:

* контроль доступа. Электронные замки позволяют контролировать, кто и когда получает доступ к определенным зонам организации. Это может помочь предотвратить несанкционированный доступ и защитить конфиденциальную информацию;
* мониторинг в реальном времени. Система видеонаблюдения позволяет наблюдать за деятельностью в организации в реальном времени. Это может помочь быстро обнаружить подозрительную активность и предотвратить возможные инциденты;
* доказательственная база, Записи с камер видеонаблюдения могут служить важными доказательствами в случае инцидентов или споров;
* профилактика преступлений. Наличие видимых камер видеонаблюдения и электронных замков может сдерживать потенциальных нарушителей, предотвращая преступления еще до их совершения;
* улучшение процедур безопасности. Анализ данных с камер видеонаблюдения и использование электронных замков может помочь организации улучшить свои процедуры безопасности, оптимизировать рабочие процессы и повысить общую эффективность.

Для обеспечения безопасности информации в информационной сфере будет далее будет рассматриваться Kaspersky Endpoint Security.

KES обеспечивает защиту в большинстве ключевых областей, что делает ее надежным решением для обеспечения информационной безопасности. В частности, KES обеспечивает защиту в следующих областях:

* идентификация и аутентификация. KES обеспечивает надежные механизмы идентификации и аутентификации, что является критически важным для предотвращения несанкционированного доступа;
* управление доступом. KES предлагает гибкие и эффективные механизмы управления доступом, позволяющие контролировать, кто и когда может получить доступ к определенным ресурсам;
* защита от вредоносного ПО. KES включает в себя современные антивирусные и антималварные механизмы для защиты от различных видов вредоносного ПО;
* системы обнаружения вторжений. KES может обнаруживать подозрительную активность или попытки вторжения, что позволяет быстро реагировать на угрозы безопасности;
* аудит и контроль. KES предоставляет инструменты для аудита и контроля, что позволяет отслеживать действия пользователей и обеспечивать соответствие политикам безопасности;
* защита информации от утечки. KES включает в себя механизмы для предотвращения утечки конфиденциальной информации;
* управление конфигурацией и изменениями. KES помогает управлять изменениями и конфигурацией системы, что является важным аспектом поддержания безопасности.

Также с помощью Kaspersky Endpoint Security (KES) можно развернуть систему резервного копирования. Это позволяет создавать резервные копии важных файлов и данных, что обеспечивает дополнительный уровень защиты от потери данных. В случае любых инцидентов, связанных с безопасностью, таких как вредоносное ПО или атаки, данные могут быть быстро восстановлены из резервной копии, минимизируя простой и потерю данных.

Межсетевой экран нужно установить перед выходом в интернет или в общедоступную зону. После установки межсетевого экрана топология сети будет выглядеть так ( рисунок 15). После установки, межсетевой экран будет служить барьером между внутренней сетью организации и внешним миром, контролируя весь входящий и исходящий трафик и блокируя любые подозрительные действия. Межсетевой экран также способен блокировать вредоносное программное обеспечение, такое как вирусы, черви и трояны, предотвращая их распространение через сеть. Это особенно важно для организаций, которые хранят конфиденциальную информацию, такую как коммерческие секреты или личные данные сотрудников. Важной функцией межсетевого экрана является контроль исходящего трафика, что позволяет предотвратить утечку конфиденциальных данных. Межсетевой экран контролирует входящий и исходящий трафик, чтобы предотвратить несанкционированную передачу информации.

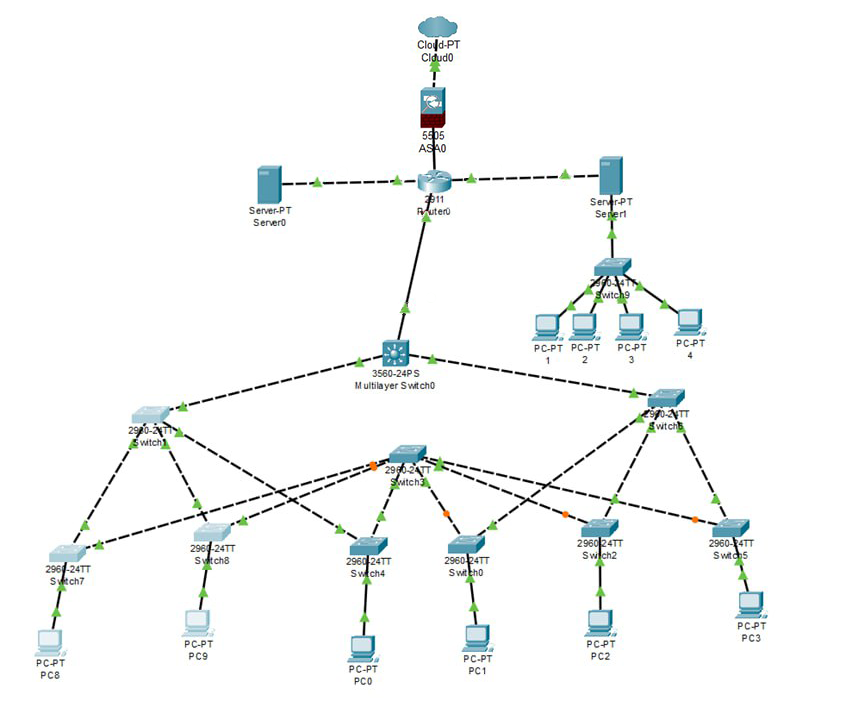


Рисунок 15 – Топология сети с межсетевым экраном.

3.2 Оценка системы защиты информации

Для оценки СЗИ будут рассмотрены различные сценарии НСД, где главной целью злоумышленника является саботаж. Это включает в себя анализ текущей СЗИ и сравнение ее с предлагаемой СЗИ. Этот подход позволяет более точно оценить эффективность предлагаемых мер безопасности и их влияние на уровень защиты информации ( рисунки 16, 17, 18 и 19).

Ситуация №1 рисунок 16).



Рисунок 16 – Ситуация несанкционированного доступа без дополнительной защиты.

На рисунке 16 изображена первая ситуация, без дополнительных электромагнитных замков и камер. У злоумышленника всего 4 шага:

* при входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу;
* злоумышленник идет в уборную, который расположен на 2 этаже;
* злоумышленник ждет 12:45, (т.к. обед с 12:30, и во время обеда все уходят и дверь остается открытой) и поднимается на 3 этаж, в 37 кабинет;
* злоумышленник беспрепятственно добрался до серверной.

Итог: в данной ситуации, злоумышленник без особых препятствий смог проникнуть в контролируемую зону и добраться до серверной комнаты. Это стало возможным из-за отсутствия дополнительных мер безопасности, таких как системы контроля доступа или видеонаблюдения. После того как злоумышленник проник в серверную, он мог совершить ряд действий, которые могут нанести серьезный ущерб инфраструктуре компании. Это может включать в себя удаление или кражу данных, установку вредоносного программное обеспечение (далее ПО) или даже физическое повреждение оборудования. Сотрудники компании обнаружат саботаж только после обеда, когда вернутся на свои рабочие места. К этому времени злоумышленник, скорее всего, уже покинет территорию компании, что значительно усложнит его поимку и приведение к ответственности.

Ситуация №2 ( рисунок 17).



Рисунок 17– Ситуация несанкционированного доступа с камерами.

На рисунке 17 изображена вторая ситуация, с камерами. У злоумышленника всего 4 шага:

* при входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу;
* злоумышленник идет в уборную, который расположен на 2 этаже;

.

* злоумышленник ждет 12:45 и поднимается на 3 этаж, в 37 кабинет;
* злоумышленник беспрепятственно добрался до серверной.

Итог: злоумышленник без особых препятствий прошел до серверной т.к. нет дополнительной защиты на прохождение в контролируемую зону. Обнаружат саботаж только после обеда, нарушителя поймают, уголовно накажут.

.

Ситуация №3 (см рисунок 18).

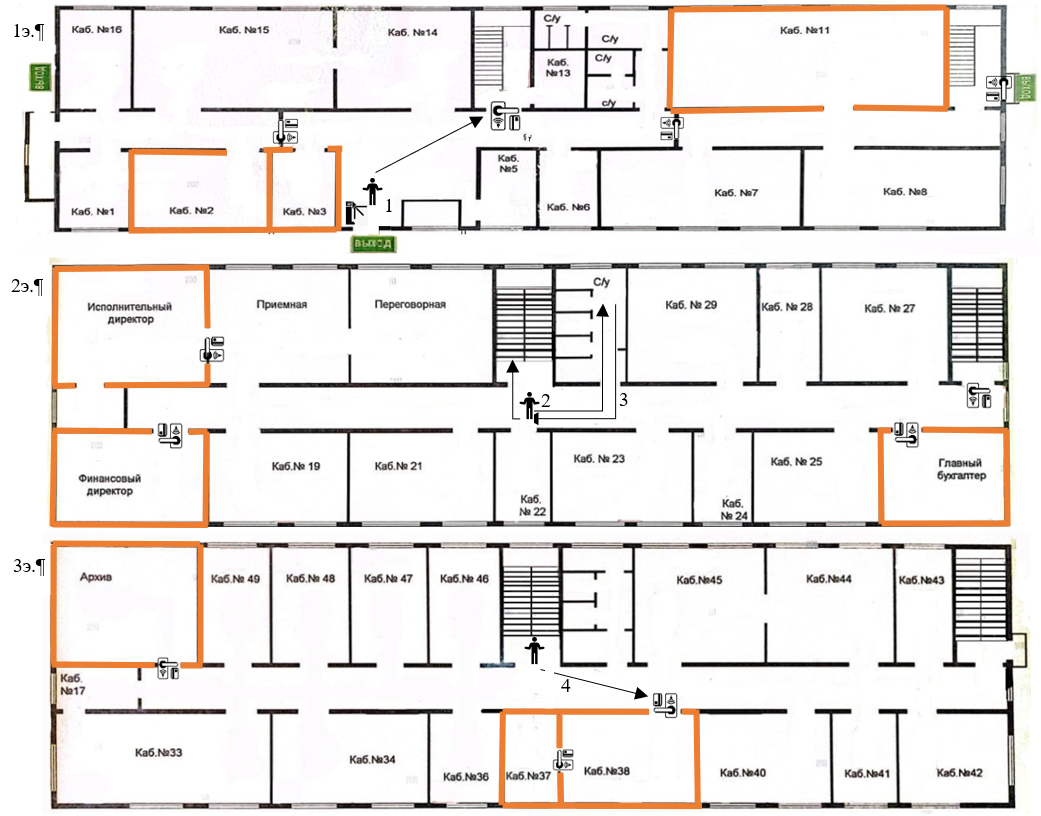


Рисунок 18 – Ситуация несанкционированного доступа с электромагнитными замками.

На рисунке 18 изображена третья ситуация, с электромагнитными замками. У злоумышленника всего 4 шага:

* при входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу;
* злоумышленник идет в уборную, который расположен на 2 этаже;
* злоумышленник ждет 12:45 и поднимается на 3 этаж;
* злоумышленник не добрался.

Итог: в данной ситуации, злоумышленник попытался проникнуть в серверную комнату, но не смог этого сделать, так как не имел необходимых для этого средств. Это говорит о том, что система безопасности работает эффективно и смогла предотвратить возможный саботаж. Однако, если у злоумышленника будет ключ-карта, он сможет обойти систему безопасности и получить доступ к серверной комнате. В этом случае, он сможет совершить саботаж, что может привести к серьезным последствиям для компании. Если злоумышленник использует ключ-карту, которая принадлежит одному из сотрудников, то вина за произошедшее будет лежать на владельце этой карты. Это подчеркивает важность ответственного отношения к средствам доступа и необходимость их надежного хранения. Несмотря на то, что злоумышленник сможет совершить саботаж, его поимка и наказание могут быть затруднены. Это связано с тем, что он может покинуть место преступления до того, как сотрудники обнаружат саботаж.

.

На рисунке 19 изображена ситуация с электромагнитными замками и камерами. У злоумышленника всего 4 шага:

* при входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу;
* злоумышленник идет в уборную, который расположен на 2 этаже;
* злоумышленник ждет 12:45 и поднимается на 3 этаж;
* злоумышленник не добрался.

Ситуация №4 ( рисунок 19).

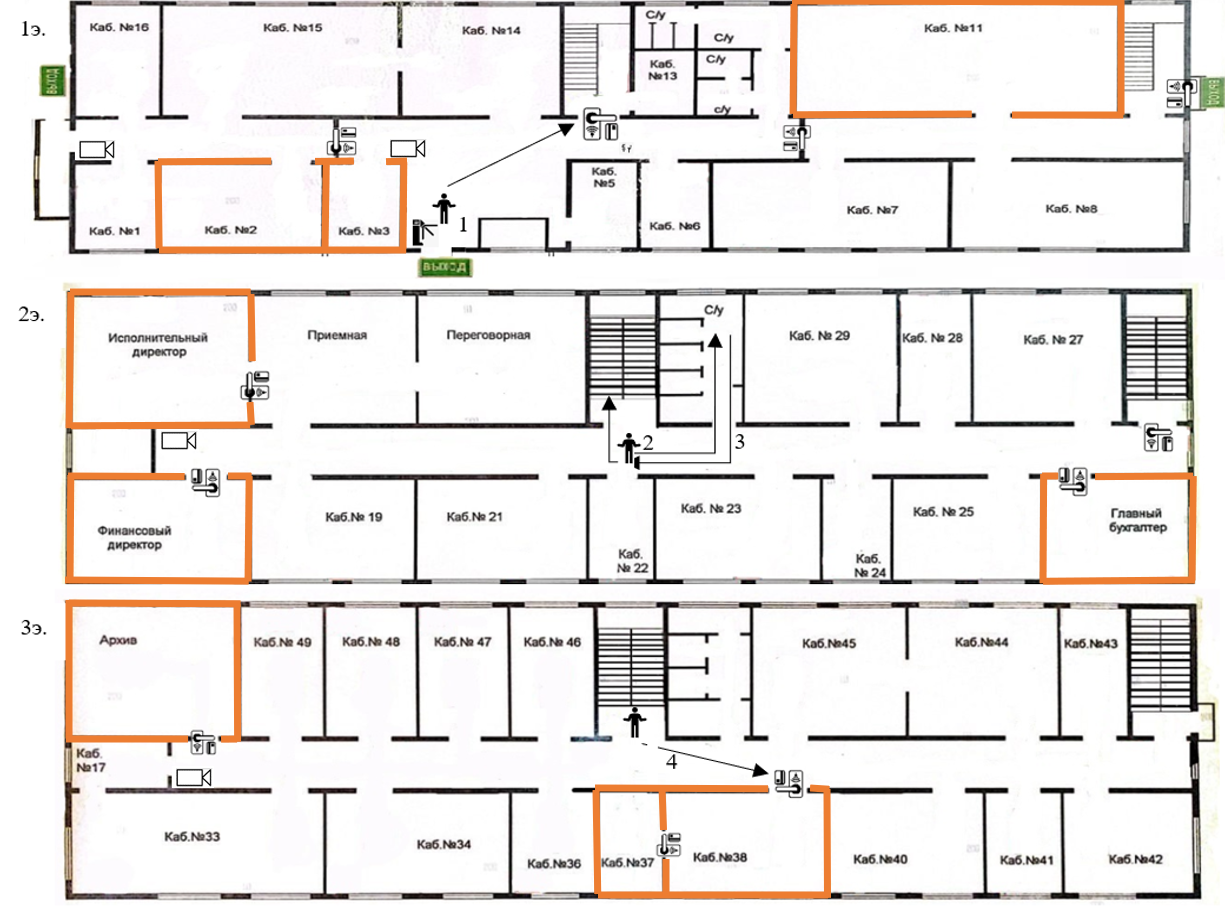


Рисунок 19 – Ситуация несанкционированного доступа с электромагнитными замками и камерами.

Итог: в данной ситуации, злоумышленник попытался проникнуть в серверную комнату, но не смог этого сделать из-за отсутствия ключ-карты. Это говорит о том, что система безопасности эффективно работает и смогла предотвратить возможный саботаж.

.

Однако, если у злоумышленника окажется ключ-карта, он сможет обойти систему безопасности и получить доступ к серверной комнате. В этом случае, он сможет совершить саботаж, что может привести к серьезным последствиям для компании.

Несмотря на возможность совершения саботажа, в данном случае у злоумышленника будет мало шансов остаться незамеченным. Благодаря системе видеонаблюдения, его действия будут зафиксированы. Это значит, что после обнаружения саботажа, сотрудники безопасности смогут просмотреть записи с камер и определить личность злоумышленника.

После того как злоумышленник будет идентифицирован, его можно будет найти и привлечь к уголовной ответственности. Это подчеркивает важность использования систем видеонаблюдения в качестве части комплексной системы безопасности.

В результате рассмотрения четырех ситуаций несанкционированного доступа были сделаны следующие выводы:

* первая ситуация: злоумышленник без особых препятствий прошел до серверной, так как нет дополнительной защиты на прохождение в контролируемую зону. Саботаж обнаружат только после обеда, когда весь персонал вернется на рабочие места. Вероятность поимки нарушителя крайне мала;
* вторая ситуация: злоумышленник также без особых препятствий прошел до серверной, однако благодаря наличию камер, его смогут обнаружить и уголовно наказать после обнаружения саботажа;
* третья ситуация: в этом случае злоумышленник не смог добраться до серверной и совершить саботаж. Однако, если у злоумышленника будет ключ-карта, он сможет проникнуть к серверной и совершить саботаж. В этом случае вина будет на владельце ключ-карты, и злоумышленник, скорее всего, не будет найден и наказан;
* четвертая ситуация: злоумышленник не смог добраться до серверной и совершить саботаж. Если у злоумышленника будет ключ-карта, он сможет проникнуть к серверной и совершить саботаж. Однако, благодаря наличию камер, его смогут обнаружить, найти и привести к уголовной ответственности.

Таким образом, наиболее эффективной является система защиты, включающая в себя как электромагнитные замки, так и камеры наблюдения. Это позволяет не только предотвратить НСД, но и обеспечить возможность идентификации и наказания нарушителя.

3.3 Экономическое обоснование

Для экономического обоснования далее будут рассмотрен оборот компании (таблица 3).

Таблица 3 – Оборот компании «Картонтара».

|  |  |
| --- | --- |
| Длительность | Сумма |
| Годовой | ~ 2,9 млрд. рублей |
| Месячный | ~ 242 млн. рублей |
| Дневной | ~ 672 тыс. рублей (672 т. картона x 1000 рублей/т) |

Данные из таблицы сконструированы на основе статистики организации за 2023год. Далее будет рассмотрена стоимость предлагаемого оборудования (таблица 4 ).

Таблица 4 – Стоимость предлагаемого оборудования.

|  |  |
| --- | --- |
| Оборудование | Сумма |
| Видеокамеры «Ginzzu HK-840N» (4 шт.) | 17990 рублей |
| Электронные замки «EM-Marine» (7 шт.) | 110481 рублей |
| Межсетевой экран «Континент 4 IPC-R1000» (1 шт.) | ~100тыс. рублей |
| Итоговая стоимость | ~228471 рублей |

В случае нарушения безопасности данных (НСД), потери могут составить более 772 тыс. рублей. Эта сумма включает в себя стоимость сервера (100 тыс. рублей) и дневной оборот (672 тыс. рублей), умноженный на количество дней, которые потребуются на восстановление системы.

Важно отметить, что возможные потери от НСД могут значительно превышать стоимость предлагаемого оборудования. Это подчеркивает важность внедрения эффективных мер безопасности для предотвращения таких инцидентов.

При этом следует учесть, что стоимость восстановления после НСД может быть значительно выше, чем просто замена оборудования или потеря дневного оборота. Возможные дополнительные затраты могут включать в себя расходы на определение и устранение уязвимостей, которые привели к НСД, а также на восстановление утраченных данных и восстановление доверия клиентов

Возможные потери от НСД значительно превышают стоимость предлагаемого оборудования.

# **ЗАКЛЮЧЕНИЕ**

В данном дипломном проекте были рассмотрены теоретические основы программно-технической защиты информации, проведен анализ организации и существующей системы защиты информации, а также нормативных документов. Были определены меры и средства защиты информации для организации, включая использование электромагнитных замков, видеокамер, приложений для удаленного доступа к рабочим местам и централизованного мониторинга систем рабочих мест.

В процессе работы были реализованы выбранные средства защиты информации, включая техническую и программную защиту. Были установлены приложения для удаленного доступа к рабочим местам и централизованного мониторинга систем рабочих мест.

В результате проведенной работы была создана эффективная система защиты информации, которая обеспечивает надежную защиту данных организации от несанкционированного доступа, модификации, искажения, копирования, блокирования или уничтожения. Это позволит организации обеспечить безопасность своей информации и уверенно развиваться в современных условиях, когда вопросы информационной безопасности становятся все более актуальными.

В дополнение к вышеуказанному, важно отметить, что в процессе работы над дипломом был проведен глубокий анализ текущих угроз безопасности, которым подвергается организация, и были предложены конкретные меры для их устранения или минимизации.

В частности, были рассмотрены такие аспекты, как защита от внешних атак, внутренние угрозы безопасности, а также риски, связанные с человеческим фактором. Были предложены методы обнаружения и предотвращения вторжений, а также меры по обеспечению физической безопасности рабочих мест.

Важной частью работы было также разработка политики безопасности и процедур, которые помогут организации поддерживать высокий уровень защиты информации в долгосрочной перспективе. Это включает в себя регулярное обучение персонала, проведение аудитов безопасности и непрерывное обновление мер и средств защиты в соответствии с изменяющимися угрозами и стандартами отрасли.

В результате этих усилий, организация не только сможет защитить свою ценную информацию, но и сохранить огромные деньги. Это, в свою очередь, способствует устойчивому росту и успеху организации в современном мире, где информационная безопасность играет все более важную роль.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Российская Федерация. Конституция Российской Федерации: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 03.04.2024).
2. Российская Федерация. Гражданский кодекс Российской Федерации: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 09.04.2024).
3. Российская Федерация. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 11.04.2024).
4. Российская Федерация. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 13.04.2024).
5. Российская Федерация. Постановление Правительства РФ от 12.04.2008 N 277 «О лицензировании деятельности по разработке, производству и распространению шифровальных (криптографических) средств, информационных систем и автоматизированных систем, защищенных с использованием шифровальных (криптографических) средств, осуществлении работ, оказанию услуг в области защиты конфиденциальной информации»: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 19.04.2024).
6. Российская Федерация. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»: текст с изменениями и дополнениями на 1 августа 2023 года. (Дата обращения: 23.04.2024).
7. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы безопасности. Системы менеджмента информационной безопасности. Требования». Дата обращения: 27.04.2024.
8. Мейерс, Э. «Сетевая безопасность». Москва: Издательство Эксмо, 2024 г. 300 стр. (Дата обращения: 01.05.2024).
9. Столлингс, У. «Компьютерная безопасность: искусство защиты». Москва: Издательство Эксмо, 2024 г. 350 стр. (Дата обращения: 03.05.2024).
10. Штамп, М. «Руководство по информационной безопасности». Москва: Издательство Эксмо, 2024 г. 400 стр. (Дата обращения: 05.05.2024).
11. Kaspersky Lab: [сайт]. – 2024г. – URL: https://www.kaspersky.ru (дата обращения: 07.05.2024)
12. Аудит информационных систем и информационной безопасности: [сайт]. – 2024г. – URL: https://www.audit-it.ru/ (дата обращения: 11.05.2024)
13. Интернет-магазин электронных замков, г. Краснодар: [сайт]. – 2024г. – URL: https://toplocks.ru (дата обращения: 23.05.2024)
14. Security Code, Межсетевой экран «Континент 4»: [сайт]. – 2024г. – URL: https://www.securitycode.ru/products/kontinent-4 (дата обращения: 11.06.2024)
15. Hrobot, Официальный интернет-магазин HOBOT: [сайт]. – 2024г. – URL: https://www.hrobot.ru (дата обращения: 12.06.2024)
16. Citilink, Официальный интернет-магазин Ситилинк: [сайт]. – 2024г. – URL: https://www.citilink.ru (дата обращения: 12.06.2024)