**СОДЕРЖАНИЕ**

[Введение 2](#_Toc167038985)

[1 Теоретические сведения по программно-технической защите информации. 4](#_Toc167038986)

[1.1 Анализ организации. 4](#_Toc167038987)

[1.2 Анализ существующей защиты информации. 5](#_Toc167038988)

[1.2.1 Определение контролируемой зоны 8](#_Toc167038989)

[1.3 Анализ нормативных документов. 8](#_Toc167038990)

[2 Проектирование системы защиты информации 10](#_Toc167038991)

[2.1 Определение мер защиты информации для организации. 10](#_Toc167038992)

[2.2 Определение средств защиты информации для организации. 11](#_Toc167038993)

[2.2.1 Электромагнитные замки. 11](#_Toc167038994)

[2.2.2 Видеокамеры. 13](#_Toc167038995)

[2.2.3 Приложения для удаленного доступа к рабочим местам. 17](#_Toc167038996)

[2.2.4 Приложения для централизованного мониторинга систем рабочих мест. 18](#_Toc167038997)

[3 Реализация средств защиты информации. 19](#_Toc167038998)

[3.1 Техническая защита. 19](#_Toc167038999)

[3.2 Программная защита. 24](#_Toc167039000)

[3.2.1 Установка приложения для удаленного доступа к рабочим местам. 24](#_Toc167039001)

[3.2.2 Установка приложения для централизованного мониторинга систем рабочих мест. 25](#_Toc167039002)

[Заключение 29](#_Toc167039003)

[Список использованных источников 30](#_Toc167039004)

# **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”. 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: − изучение основных принципов защиты информации и их применение на производственных объектах; − анализ существующих систем защиты информации, выявление их преимуществ и недостатков; − разработка собственной системы защиты информации с использованием современных программно-технических средств; − проведение экспериментов для оценки надежности и эффективности разработанной системы.

На сегодняшний день существует множество систем защиты информации, 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 системы защиты.

Объектом исследования являются системы защиты информации на производственных объектах.

Предметом исследования выступает разработка программно-технических мероприятий по защите информации на объекте ООО «Картонтара».

Разработка эффективной системы защиты информации 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 системы защиты для оценки эффективности разработанной системы.

# **1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ПРОГРАММНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ.**

## **1.1 Анализ организации.**

Компания SFT Group (далее «Картонтара») – это ведущий производитель гофроупаковки и макулатурного картона в России.

В организации хранятся данные о работниках и производственные данные, отсюда следует, что Картонтара имеет 4 уровень защищенности

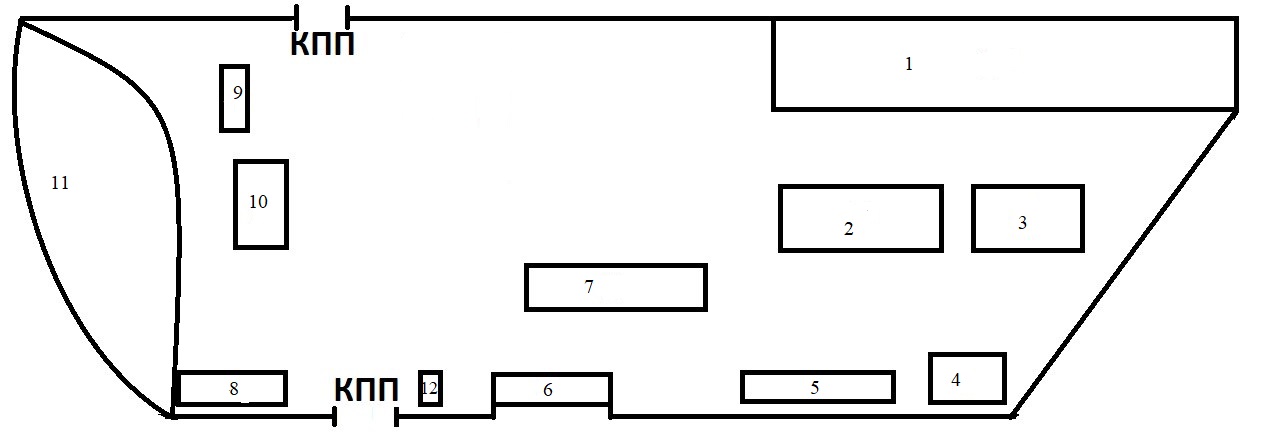
На территории Картонтары располагаются множество зданий. В каждом здании выполняют различные функции. Всего зданий на территории 11 (см. рисунок 1).

Рисунок 1 - План территории «Картонтары».

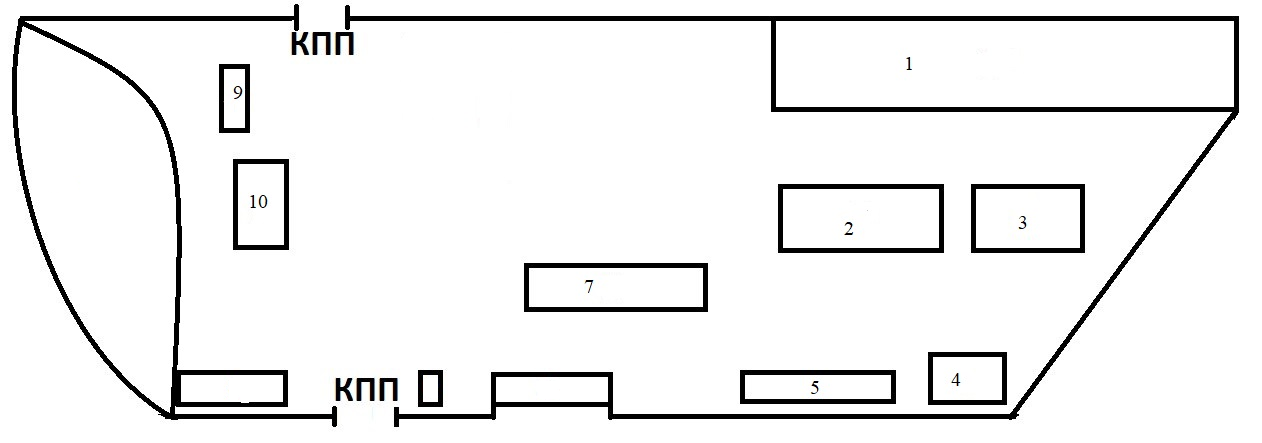
На Рисунке 1 изображен план территории «Картонтары»: здания, входы/выходы. Все здания можно разделить на 2 группы: «Офисные» и «Производственные». (см. рисунок 2).

Рисунок 2 - Производственные здания

На рисунке 2 выделены производственные здания.

«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 5» является складом для сырья.

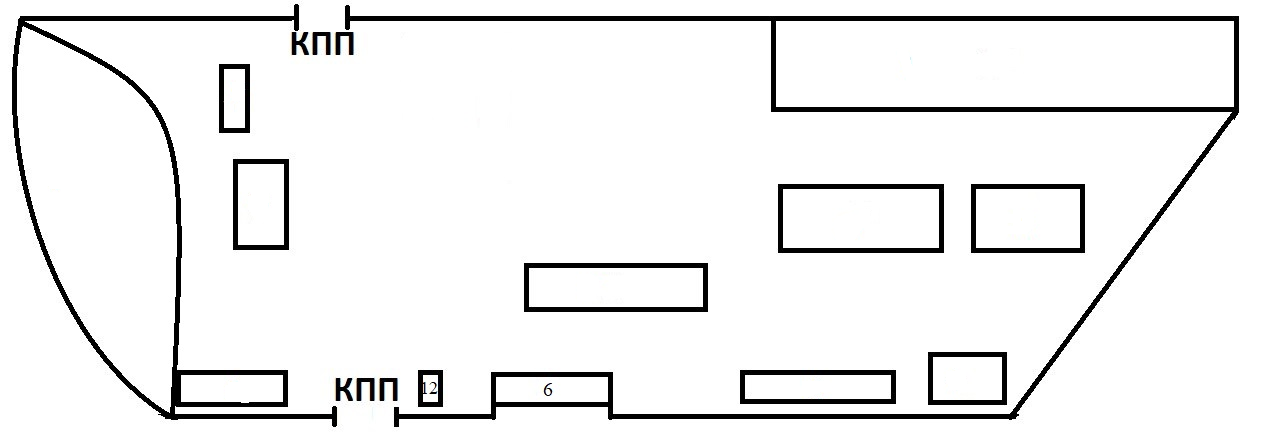
Ниже рассмотрены офисные здания (см. Рисунок 3).

Рисунок 3 - Офисные здания

На рисунке 3 выделены «офисные здания». Здания, куда приходит/хранится/обрабатывается вся информация.

«Здание 6» является главным зданием, в задании 6, происходит все манипуляции с информацией.

## **1.2 Анализ существующей защиты информации.**

В организации присутствует система управления доступа (СКУД). С помощью данной системы охрана видит кто и куда прошел. В кабинете и установлен данный сервер контроля доступом.

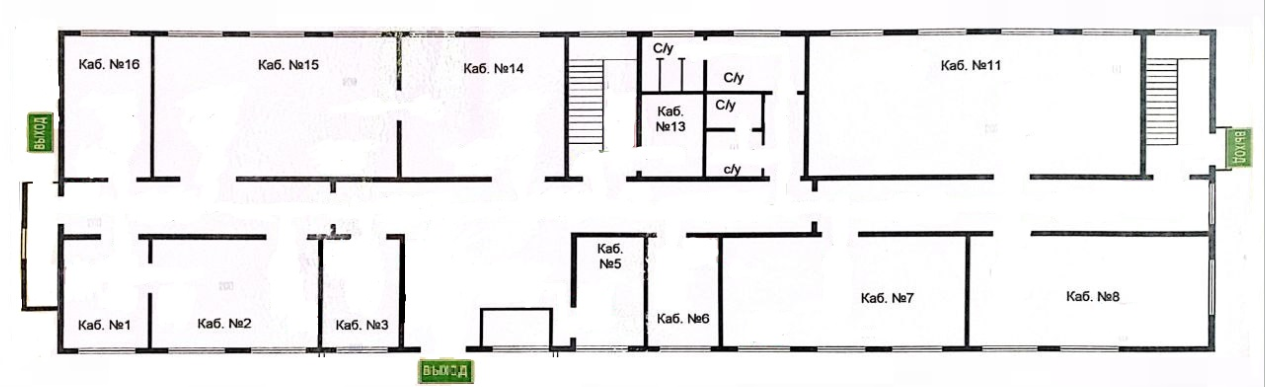
Ниже будет рассмотрено подробнее «Здание 6», оно имеет 3 этажа. (см. рисунок 4).

Рисунок 4 - 1й этаж «Здания 6».

На рисунке 4 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.

Кабинет №3 является кабинетом охраны.

В данном кабинете присутствует окошко в сторону турникета. Если, у человека который захочет пройти внутрь и не будет электронного пропуска, он попросит документ удостоверяющий документ и пропустит, и откроет дверь в случае надобности.

В кабинете №3 стоит компьютер с такими характеристиками:

* материнская плата: ASUS;
* процессор Intel Corei5-3470 CPU @ 3.20GHz3.60GHz;
* оперативная память (RAM): 32 ГБ;
* жесткий диск (HDD): 80 ГБ;
* тип привода: DVD+/-RW.

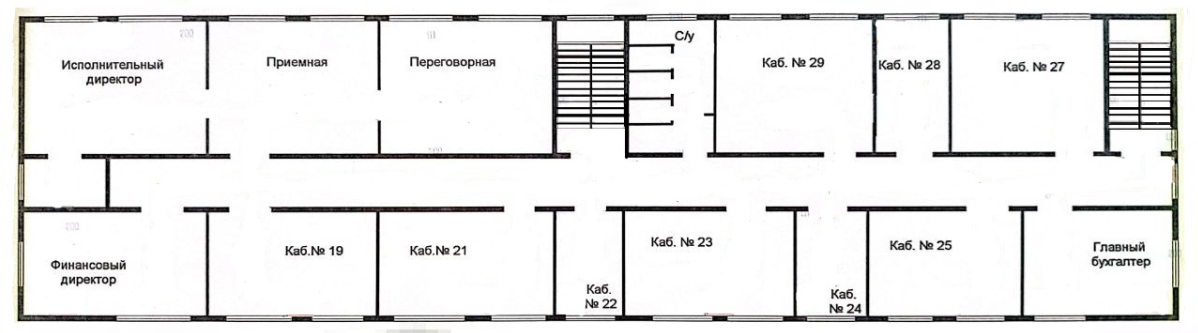
Ниже будет рассмотрен 2й этаж: (см. рисунок 5).

Рисунок 5 - 2й этаж «Здания 6».

На рисунке 5 изображен 2й этаж плана «Здания :6». Здесь отсутствуют электронные замки и другие физические препятствия.

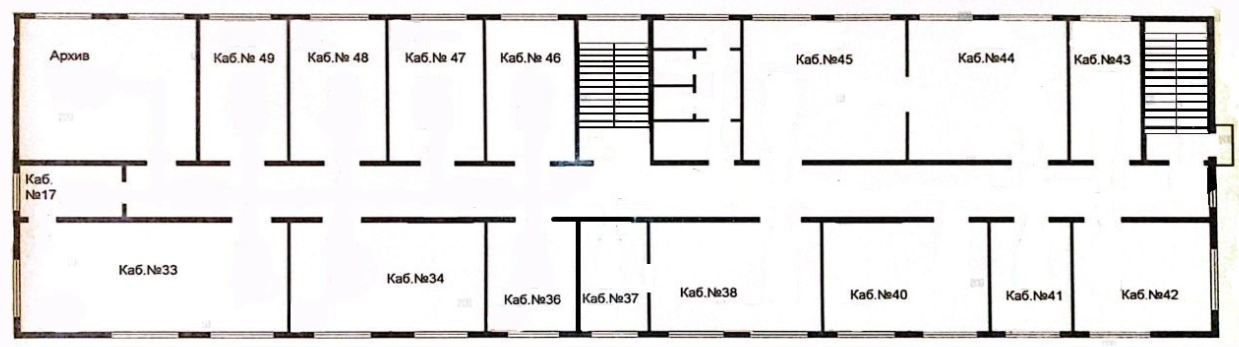
Ниже будет рассмотрен 3й этаж: (см. рисунок 6).

Рисунок 6 - 3й этаж «Здания 6».

На рисунке 6 изображен 3й этаж. Здесь также как и на втором этаже отсутствуют дополнительные физические барьеры.

Кабинет №37 является серверной.

Кабинет №38 является комнатой системных администраторов.

.В кабинете №37 стоят сервера, но на вход и выход нет дополнительной защиты. На серверах хранятся данные которые приходят из компьютеров из производственных зданий.

В кабинете №38 стоят 4 работающих компьютеров администраторов, со следующими характеристиками:

* материнская плата: ASUS;
* процессор Intel Corei5-3470 CPU @ 3.20GHz3.60GHz;
* оперативная память (RAM): 32 ГБ;
* жесткий диск (HDD): 80 ГБ;
* тип привода: DVD+/-RW.

В кабинете №38 осуществляются такие задачи как :

* 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.

Также системные администраторы в случае поломки какого-либо компьютера (системной поломки) должны идти к проблемному компьютеру. Нет централизованного управления и мониторинга рабочих мест.

### **1.2.1 Определение контролируемой зоны**

Отсюда следует, что в офисе есть кабинеты, которые должны быть максимально защищены от несанкционированного доступа.

Кабинеты критической важности:

* кабинет №2;
* кабинет №3;
* кабинет №11;
* кабинет Исполнительного директора;
* кабинет финансового директора;
* кабинет главного бухгалтера;
* кабинет №37;
* кабинет №38.

Внутри данных кабинетов обрабатывается информация, поэтому критически важно поставить дополнительную защиту на вход.

## **1.3 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.

# **2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

## **2.1 Определение мер защиты информации для организации.**

В прошлой главе, была рассмотрена территория и офисное здание «картонтары». Я нашел недочеты в безопасности, чтобы их закрыть я предлагаю совершить следующие этапы:

* установить электронные замки на входах в контролируемую зону. Это поможет контролировать доступ к определенным зонам здания. Электронные замки могут быть настроены так, чтобы только определенные сотрудники могли получить доступ, что повысит уровень безопасности;
* установить видеокамеры с полем видимости на подходы к контролируемой зоне. Видеонаблюдение является важным элементом системы безопасности. Оно позволяет мониторить активность и может быть использовано для идентификации подозрительной активности;
* установить приложения для удаленного доступа к рабочим местам. : Это позволит сотрудникам работать из любого места, что может быть особенно полезно в условиях пандемии или других экстренных ситуаций;
* установить приложения для централизованного мониторинга систем рабочих мест. Это позволит IT-отделу эффективно отслеживать и управлять всеми рабочими станциями. Они смогут быстро обнаруживать и устранять любые проблемы, что поможет минимизировать простои и повысить производительность.

Прохождение данных этапов, и регулярное использование этих аспектов одновременно может привести к созданию голистической системы безопасности, которая обеспечивает защиту на всех уровнях.

* физическая безопасность: электромагнитные замки и видеокамеры обеспечивают физическую безопасность здания. они контролируют доступ к зданию и его различным зонам, а также позволяют мониторить активность вокруг здания.
* программная безопасность: приложения для удаленного доступа и централизованного мониторинга обеспечивают защиту данных. они позволяют сотрудникам безопасно получать доступ к рабочим местам из любого места и обеспечивают it-отделу возможность эффективно отслеживать и управлять всеми рабочими станциями.

## **2.2 Определение средств защиты информации для организации.**

Для того чтобы закрыть этапы, которые описаны выше, в данной работе рассматриваются следующие аспекты:

Установка электромагнитных замков.

Установка видеокамер.

Установка приложений для удаленного доступа.

Установка приложений для централизованного мониторинга.

### **2.2.1** **Электромагнитные замки.**

Электромагнитные замки практически полностью исключают возможность несанкционированного доступа к личным вещам и документам хранящимся в шкафчиках и ящиках рабочего стола.

****Для предотвращения несанкционированного доступа далее будет рассматриваться электронный замок TL-108. (см. рисунок 7)

Рисунок – 7 электромагнитный замок TL-108.

На рисунке 7 изображен электронный замок TL-108. С такими характеристиками:

* материал: цинковый сплав;
* цвет: серебро, золото;
* источник питания: 4 щелочных элемента, типоразмер aa;
* время работы от источника питания: 11-12 месяцев;
* доступ: rfid-браслет, брелок;
* сфера применения: школы, спа-салоны, сауны, спортивные залы, гостиницы, офисы и т.д.

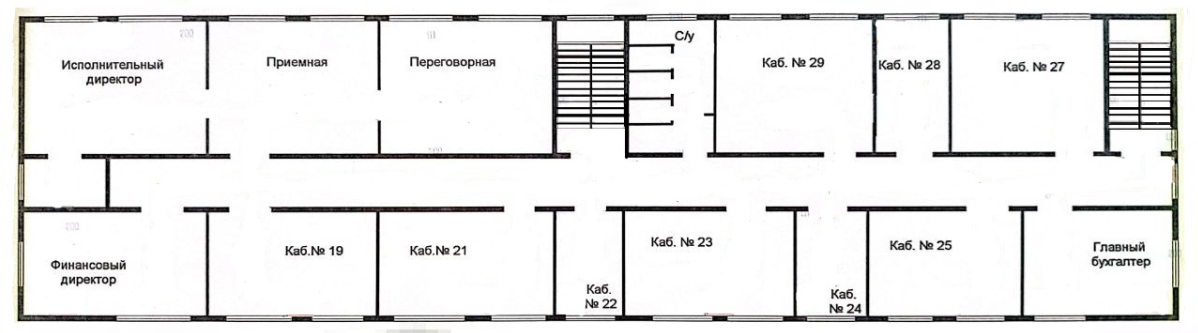
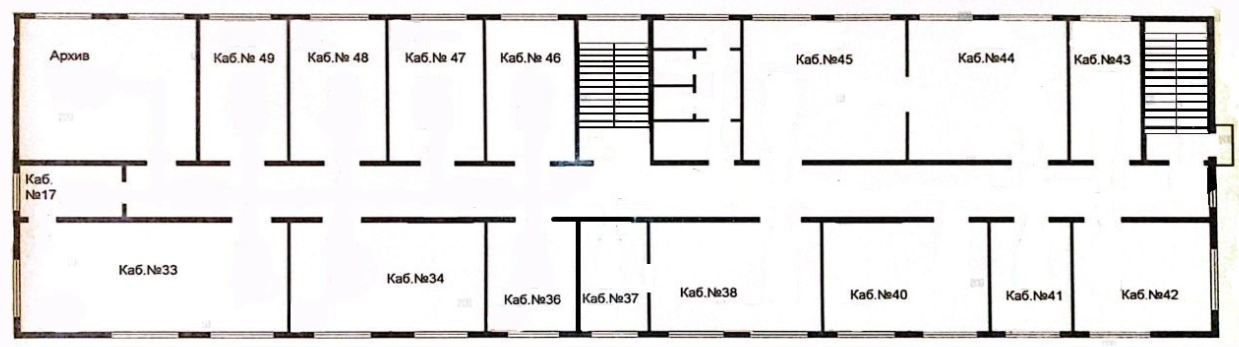
Далее будут рассмотрены этажи с дополнительными электромагнитными замками на рисунках 8 и 9.

Рисунок 8 – Второй этаж с электронными замками.

Рисунок 9 – Третий этаж с электронными замками.

Электронные замки стоят на вход в контролируемую зону. Также данные замки нужно подключить к существующей СКУД, чтобы можно было записывать данные о перемещении.

Использование таких замков дает

* электронные замки помогают предотвратить несанкционированный доступ 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.

### **2.2.2 Видеокамеры.**

Использование видеокамер в случае происшествия, поможет определить время нарушения и личность нарушителя. Также полезны по следующим причинам:

* видеокамеры могут помочь обеспечить безопасность сотрудников, отслеживая любые подозрительные действия или нежелательные посетители;
* видеонаблюдение может помочь предотвратить кражу или вандализм, позволяя оперативно реагировать на подобные инциденты;
* видеокамеры могут помочь контролировать соблюдение правил и процедур организации, особенно на производственных площадках, где безопасность является приоритетом;
* в случае конфликтов или спорных ситуаций видеозаписи могут служить доказательной базой;

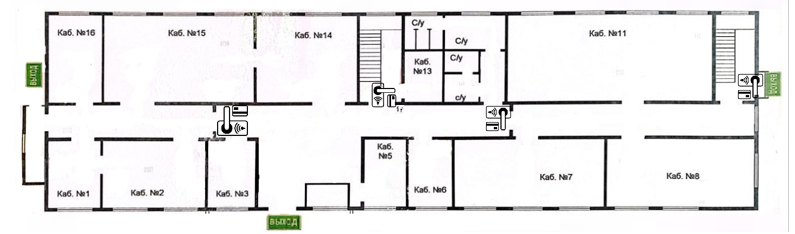
Для постоянного мониторинга над ситуацией внутри помещения и в случае какого-либо нарушения идентификации нарушителя будет предложено использовать видеокамеру Ginzzu HK-840N. (см. рисунок 10).

Рисунок 10 – Видеокамера Ginzzu HK-840N.

На рисунке 10 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.

Далее будут рассмотрены этажи с камерами на рисунках 11, 12 и 13.

Рисунок 11 - Улучшенный первый этаж

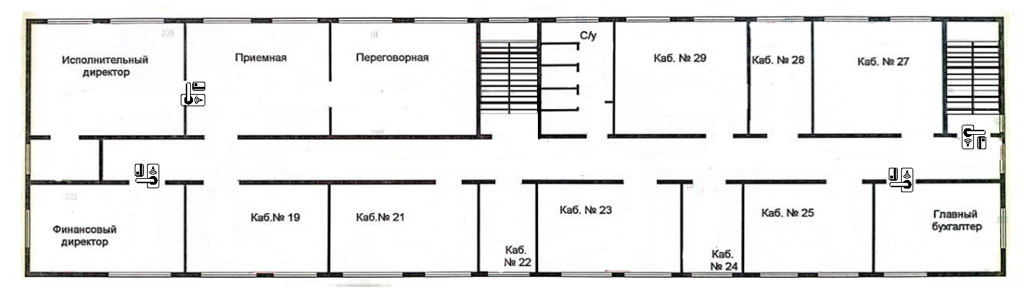
Камера с номером 1 должна видеть все входы. Камера с номером 2 должна видеть два входа с электромагнитными замками 2 входа без электромагнитных замков.

Рисунок 12 – Улучшенный второй этаж.

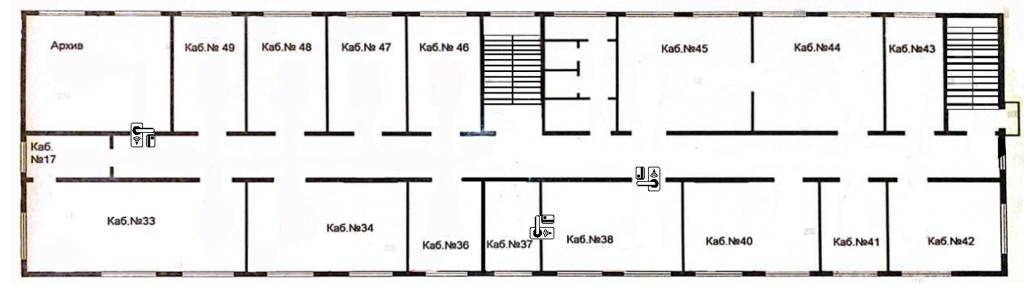
На втором этаже достаточно одной камеры, ведь на втором этаже нет дверей посреди коридоров. Но камера должна захватывать полностью коридор.

Рисунок 13 – Улучшенный третий этаж.

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

### **2.2.3 Приложения для удаленного доступа к рабочим местам.**

Чтобы закрыть данный аспект будет рассматриваться отечественная программа «Ассистент».

«Ассистент» – это высокотехнологичный программный продукт российского производства, который обеспечивает безопасный удаленный доступ к компьютерам по локальной сети или через Интернет. Широкие возможности совместно с простотой использования делают «Ассистент» незаменимым помощником при решении широкого круга задач: от удаленной работы до администрирования серверов. У «Ассистента» есть такие возможности как:

Удаленное управление рабочим столом:

* просмотр экранов удаленного компьютера;
* поддержка горячих клавиш;
* синхронный буфер обмена;
* перехват управления удаленным компьютером;
* групповое подключение к удаленному компьютеру;
* поддержка мультимониторных систем;
* блокировка устройств ввода;
* работа с несколькими удаленными компьютерами одновременно.

Настройка удаленного компьютера:

* обмен файлами;
* редактор реестра;
* диспетчер задач;
* диспетчер устройств;
* командная строка;
* управление питанием;
* удаленная печать;
* wake-оn-LAN.

Коммуникации:

* текстовый чат;
* аудио и видео чаты;
* графические заметки на удаленном экране.

### **2.2.4 Приложения для централизованного мониторинга систем рабочих мест.**

Для закрытия вопроса централизованного мониторинга всех систем, будет рассматриваться Kaspersky Security Center.

KSC позволяет не только централизованно следить за компьютерами, но также и обеспечивает защиту, т.к. он еще устанавливает антивирус, KASPERSKY ENDPOINT SECURITY.

Kaspersky Endpoint Security для Windows включает передовую многоуровневую защиту от угроз, проактивные технологии, такие как Контроль программ, Веб-Контроль и Контроль устройств, средства управления уязвимостями и установкой исправлений, а также шифрование данных. Вот только некоторые преимущества приложения:

* защита наиболее ценных активов компании – данных, репутации и непрерывности бизнес-процессов;
* эффективное администрирование – развертывание и управление выполняются из единой консоли с применением общих политик;
* надежная защита, эффективность которой доказана независимыми тестами;
* инновационные исследования и стратегия разработки – мы сами создаем все наши технологии, что позволяет нам с легкостью интегрировать их в наши продукты;
* совместимость с существующими инфраструктурами.

# **3 РЕАЛИЗАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.**

## **3.1 Техническая защита.**

Далее будет рассмотрена ситуация несанкционированного доступа. Где главная цель злоумышленника это -саботаж, с разными условиями, на рисунках 14, 15, 16 и 17.

Ситуация №1 (см. рисунок 14).

Рисунок 14 – Ситуация несанкционированного доступа без

дополнительной защиты.

На рисунке 14 изображена первая ситуация без дополнительных электромагнитных замков и камер. Всего 4 шага:

1. При входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу.
2. Злоумышленник идет в туалет, который расположен на 2 этаже.
3. 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.
4. 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, когда весь персонал вернется на рабочие места, нарушителя вряд-поймают.

.

Ситуация №2 (см. рисунок 15).

Рисунок 15 – Ситуация несанкционированного доступа с камерами.

На рисунке 15 изображена вторая ситуация, с камерами. Всего 4 шага:

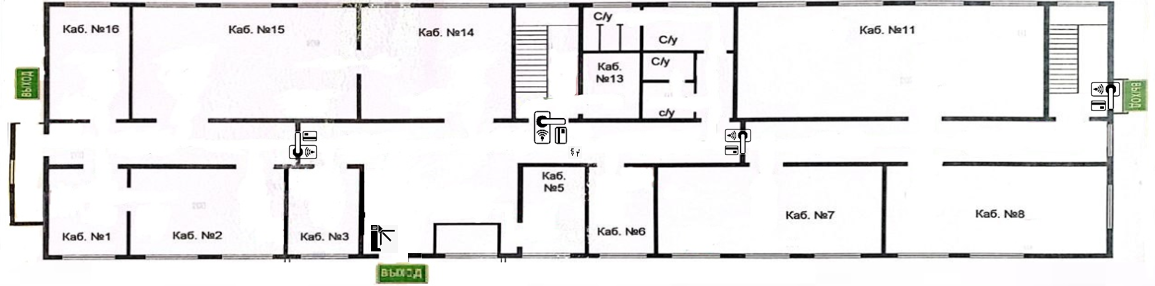
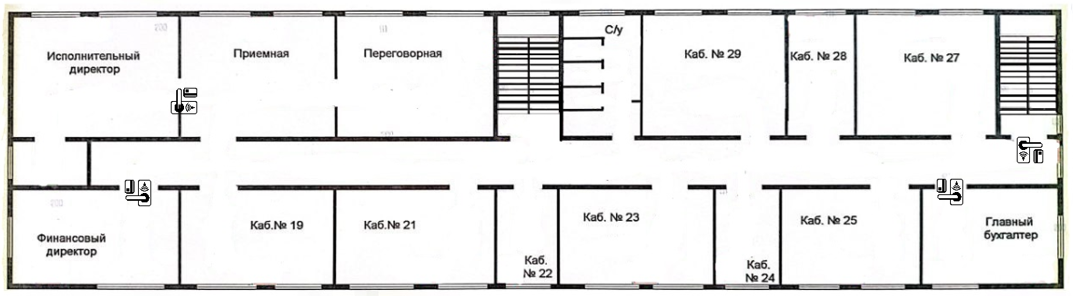
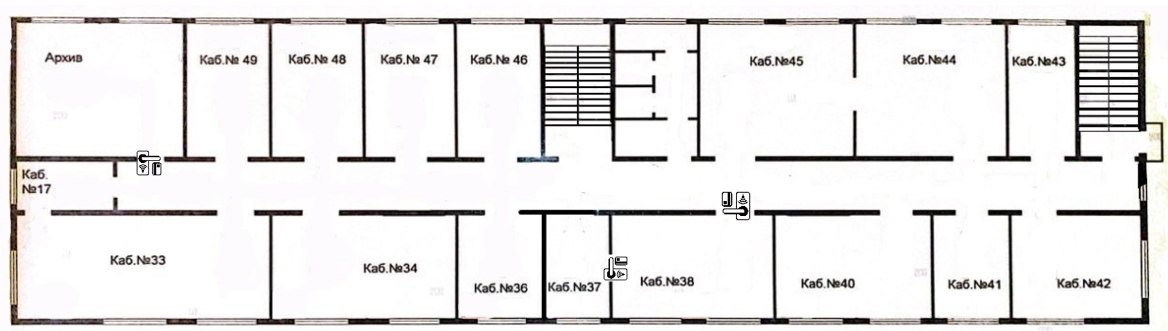
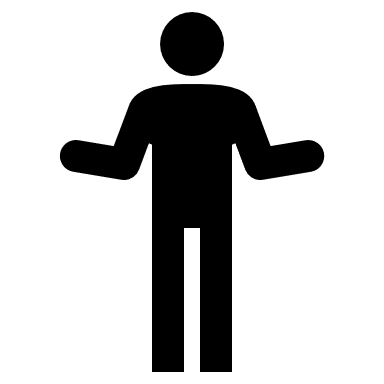
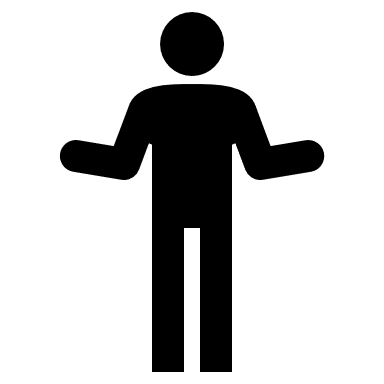
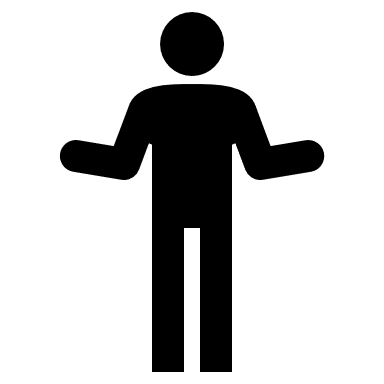
1. При входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу.
2. Злоумышленник идет в туалет, который расположен на 2 этаже.

.

1. Злоумышленник ждет 12:45 и поднимается на 3 этаж, в 37 кабинет.
2. 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 16).

4.

2.

3.

1.

3э.

2э.

1э.

Рисунок 16 – Ситуация несанкционированного доступа с электромагнитными замками.

На рисунке 16 изображена третья ситуация, с электромагнитными замками. Всего 4 шага:

1. При входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу.
2. Злоумышленник идет в туалет, который расположен на 2 этаже.
3. Злоумышленник ждет 12:45 и поднимается на 3 этаж.
4. Злоумышленник не добрался.

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. С помощью СКУД теперь видно время прихода и отхода сотрудников.

Итог: злоумышленник не добрался до серверной и не смогу совершить саботаж. Но если у злоумышленника будет ключ карта, то он сможет проникнуть к серверной и совершить саботаж. И тогда вина будет на хозяине ключ карты и злоумышленник опять не будет найден и наказан.

.

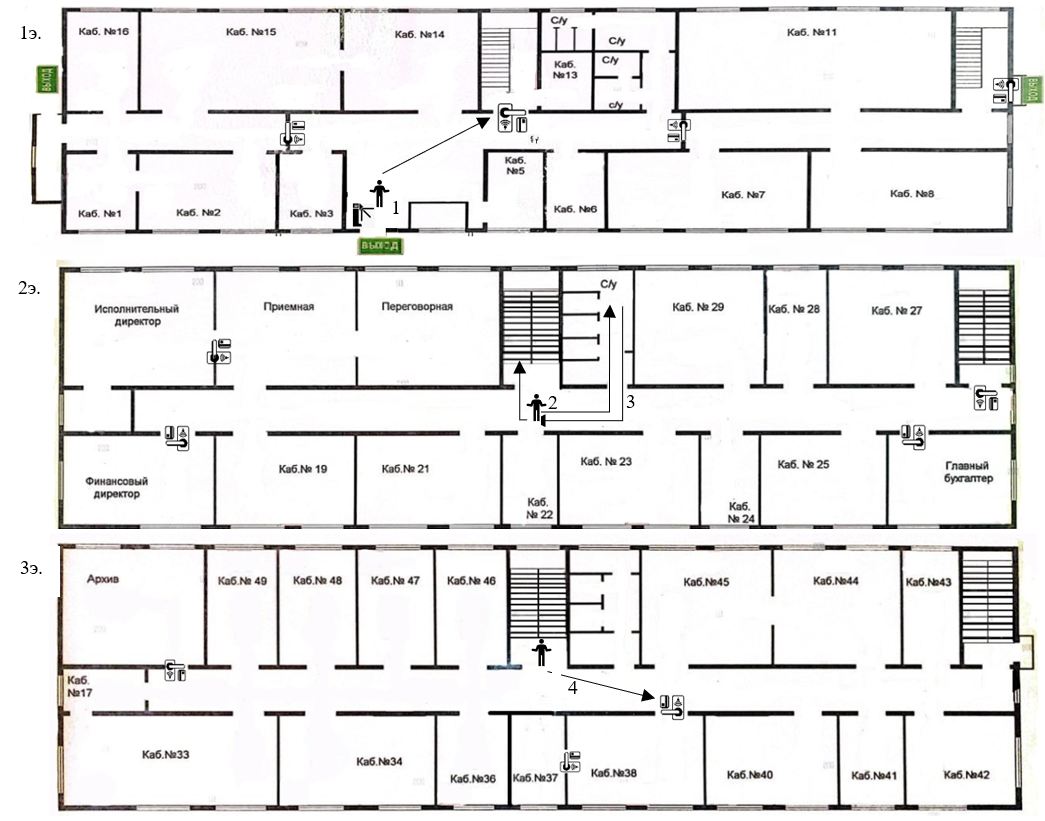
Ситуация №4 (см. рисунок 17).

Рисунок 17 – Ситуация несанкционированного доступа с электромагнитными замками и камерами.

На рисунке 17 изображена ситуация с электромагнитными замками и камерами. Всего 4 шага:

1. При входе злоумышленник, дает документ и просит открыть дверь ведущую на лестницу.
2. Злоумышленник идет в туалет, который расположен на 2 этаже.
3. Злоумышленник ждет 12:45 и поднимается на 3 этаж.
4. Злоумышленник не добрался.

Итог: злоумышленник не добрался до серверной и не смогу совершить саботаж. Но если у злоумышленника будет ключ карта, то он сможет проникнуть к серверной и совершить саботаж. Но его обнаружат по камерам, и смогут найти и привести к уголовной ответственности.

.

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

* 1 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;
* 2 ситуация: злоумышленник также без особых препятствий прошел до серверной, однако благодаря наличию камер, его смогут обнаружить и уголовно наказать после обнаружения саботажа;
* 3 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;
* 4 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 несанкционированный доступ, но и обеспечить возможность идентификации и наказания нарушителя.

## **3.2 Программная защита.**

### **3.2.1 Установка приложения для удаленного доступа к рабочим местам.**

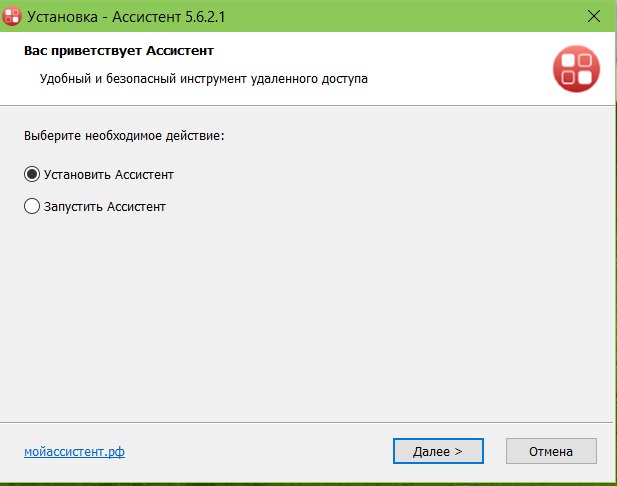
Программу «АССИСТЕНТ» достаточно легко установить как и опытному пользователю ПК, так и недельному пользователю. Есть две версии программы, для постоянного использования и для единичного раза. (см. рисунок 18).

Рисунок 18 – загрузочное окно ассистента.

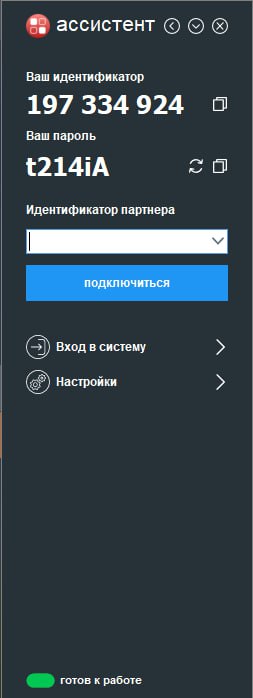
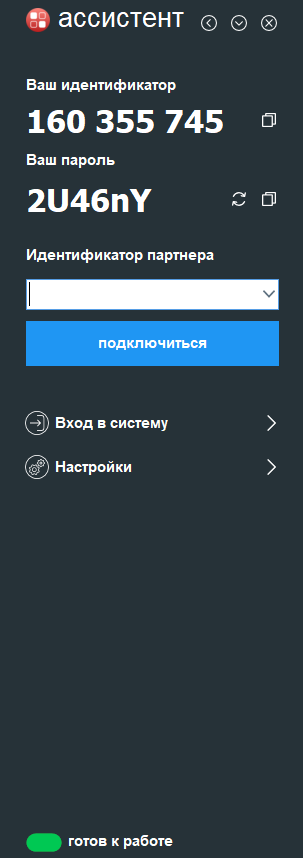
После установки откроется окно с уникальным идентификатором (адресом для подключения). И паролем на подключение (см. рисунок 19). Чтобы компьютер «А», подключился к компьютеру «Б», в графе «Идентификатор партнера» нужно вписать идентификатор компьютера «Б» (160355745), а в графе «Пароль партнера»(2U46nY).

Рисунок 19 – окно приложения «АССИСТЕНТ».

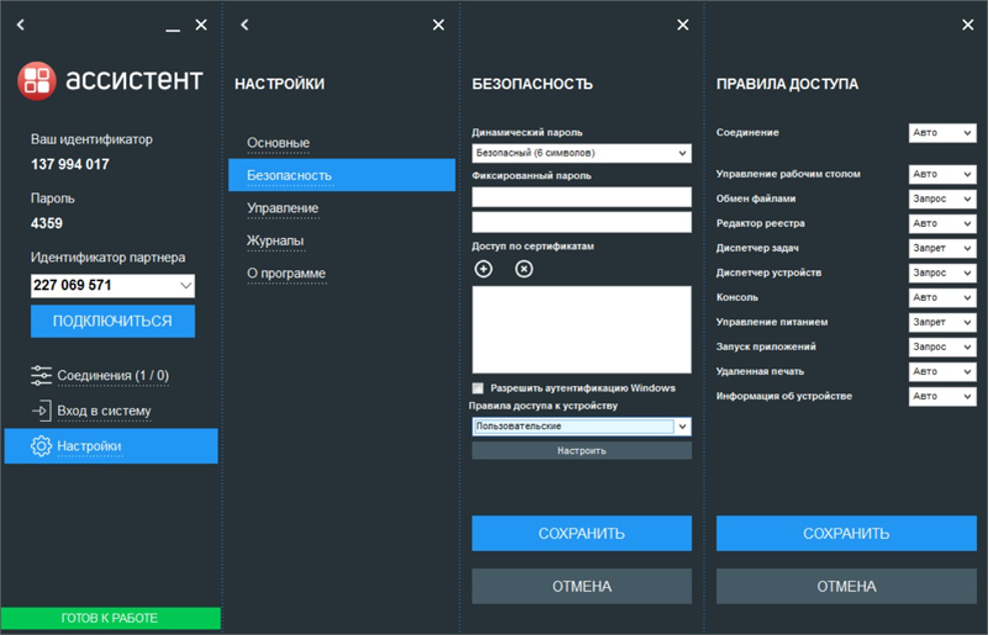
У приложения есть свои настройки для настройки безопасности. (см. рисунок 20).

Рисунок 20 – настройки безопасности «АССИСТЕНА».

Теперь системные администраторы в случае сбоев или других инцидентов могут быстро реагировать, получив удаленный доступ к нужной системе, также могут управлять серверами организации на расстоянии

### **3.2.2 Установка приложения для централизованного мониторинга систем рабочих мест.**

Установить KSC уже достаточно сложно. Рекомендуется пользоваться учебным пособие, которое есть на YouTube канале «Kaspersky». В нем подробно рассматривается каждый пункт. Помимо установки там разбирается и настройка безопасности. После завершения установки и настройки KSC на компьютере системного администратора, KSC увидит все компьютеры которые находятся в сети, и установит на них KES (Kaspersky Endpoint Security), с помощью которого KSC и может мониторить все системы (см. рисунок 21).

Рисунок 21 – работа KSC.

. После установки через компьютер, на котором установлен KSC можно будет мониторить все системы. Все подозрительные действия будут показаны на компьютере системного администратора (см. рисунок 22).

Рисунок 22 – KSC окно мониторинга.

Данное окно мониторинга позволяет:

* получать обзор состояния системы;
* получать оповещения о критических проблемах;
* просматривать список последних событий;
* обеспечивать безопасность.

Панель мониторинга предоставляет обзор состояния и производительности системы в реальном времени. Виджеты и графики отображают данные о загрузке процессора, использовании памяти, сетевой активности и т.д.

Система может автоматически генерировать оповещения о критических проблемах, что позволяет администратору быстро реагировать и предотвращать возможные сбои.

Панель также отображает список последних событий, что помогает в быстрой диагностике и устранении проблем.

При правильной настройке, система мониторинга может служить дополнительным слоем защиты, позволяя администратору отслеживать любые необычные или подозрительные действия в системе.

После установки Kaspersky Security Center, системным администраторам открываются следующие возможности:

* KSC предоставляет мощную консоль управления с дополнительным гибким веб-интерфейсом, доступным в любом месте с любого стационарного или мобильного устройства.
* KSC позволяет просматривать параметры безопасности и управлять защитой во всей корпоративной среде, включая облачные, физические и виртуальные машины, а также мобильные устройства.
* с помощью готовых к использованию унифицированных политик, KSC облегчает развертывание и управление безопасностью.
* KSC позволяет управлять уязвимостями и обновлениями программ на компьютерах сети.
* KSC формирует подробное представление об аппаратном и программном обеспечении в вашей сети, что позволяет экономить на лицензировании благодаря централизованному мониторингу и предоставлению прав на использование.

# **ЗАКЛЮЧЕНИЕ**

В данной дипломной работе 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.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Мейерс, Э. «Сетевая безопасность»: книга / Э. Мейерс. – 2024г.
2. Столлингс, У. «Компьютерная безопасность: искусство защиты»: книга / У. Столлингс. – 2024г.
3. Штамп, М. «Руководство по информационной безопасности»: книга / М. Штамп. – 2024г.
4. Kaspersky Lab: [сайт]. – 2024г. – URL: https://www.kaspersky.ru (дата обращения: 23.03.2024)
5. АССИСТЕНТ | Удаленный доступ, управление и администрирование: [сайт]. – 2024г. – URL: https://xn–80akicokc0aablc.xn–p1ai
6. Интернет-магазин электронных замков, г. Краснодар: [сайт]. – 2024г. – URL: https://toplocks.ru.
7. Использование биометрии в информационной безопасности // URL: https://web.snauka.ru/issues/2023/09/100808 (дата обращения: 23.03.2024)
8. Роль биометрических технологий в современном контроле доступа // URL: https://manggis.kz/blog/rol\_biometricheskih\_tehnologij\_v\_sovremennom\_kontrole\_dostupa (дата обращения: 23.03.2024)
9. Биометрия. Стандарты. Технологии. Задачи. Решения // URL: http://www.techportal.ru/security/biometrics (дата обращения: 18.04.2024)
10. Биометрические системы защиты - виды, особенности // URL: https://tatprofing.com/blog/biometricheskie-sistemy-zashhity (дата обращения: 23.03.2024)
11. Обзор и анализ биометрической системы защиты // URL: https://scienceforum.ru/2017/article/2017036036 (дата обращения: 18.04.2024)
12. Биометрические данные: как собираются, хранятся и обрабатываются // URL: https://gb.ru/blog/biometricheskie-dannye (дата обращения: 18.04.2024)
13. Биометрия - типы и тенденции // URL: https://www.intelvision.ru/blog/biometricheskaya\_identifikaciya (дата обращения: 18.04.2024)
14. Какие бывают типы биометрических датчиков // URL: https://bing.com/search?q=%d0%a2%d0%b8%d0%bf%d1%8b+%d0%b1%d0%b8%d0%be%d0%bc%d0%b5%d1%82%d1%80%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8%d1%85+%d0%b4%d0%b0%d0%bd%d0%bd%d1%8b%d1%85 (дата обращения: 18.04.2024)
15. Биометрия: что такое биометрические данные человека, как их собирают // URL: https://skillbox.ru/media/code/biometricheskie-dannye-chto-eto-takoe-i-gde-khranitsya-biometriya (дата обращения: 18.04.2024)
16. Что такое биометрические данные и зачем они нужны // URL: https://news.rambler.ru/tech/52161859-chto-takoe-biometricheskie-dannye-i-zachem-oni-nuzhny (дата обращения: 18.04.2024)
17. Биометрия: как технология распознавания личности меняет мир // URL: https://bing.com/search?q=%d0%9f%d1%80%d0%b8%d0%bd%d1%86%d0%b8%d0%bf%d1%8b+%d1%80%d0%b0%d0%b1%d0%be%d1%82%d1%8b+%d0%b1%d0%b8%d0%be%d0%bc%d0%b5%d1%82%d1%80%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8%d1%85+%d1%81%d0%b8%d1%81%d1%82%d0%b5%d0%bc (дата обращения: 18.04.2024)
18. Биометрия человека: понятие и принципы работы // URL: https://obzorposudy.ru/polezno/cto-takoe-biometriya-celoveka-i-kak-ona-rabotaet (дата обращения: 18.04.2024)
19. Обзор инновационных технологий в области биометрии // URL: https://otzyvysotrudnikov.ru/obzor-innovacionnih-tehnologiy-v-oblasti-biometrii (дата обращения: 05.05.2024)
20. Биометрический замок - обзор, характеристики, виды и отзывы // URL: https://www.syl.ru/article/328669/biometricheskiy-zamok—obzor-harakteristiki-vidyi-i-otzyivyi (дата обращения: 05.05.2024)
21. Идентификация человека по биометрическим данным: обзор современных // URL: https://cyberleninka.ru/article/n/identifikatsiya-cheloveka-po-biometricheskim-dannym-obzor-sovremennyh-tehnologiy (дата обращения: 05.05.2024)
22. Современные биометрические методы идентификации // URL: https://habr.com/ru/articles/126144 (дата обращения: 05.05.2024)
23. Биометрические технологии на службе современного мира // URL: https://spravochnick.ru/informacionnye\_tehnologii/biometricheskie\_tehnologii\_na\_sluzhbe\_sovremennogo\_mira (дата обращения: 05.05.2024)