Содержание

Введение 3

1 Назначение и цели построения системы 4

2 Описание предметной области 5

2.1 Описание объекта информатизации 5

4 Постановка задачи 12

4.1 Система инженерно-технической защиты 13

5 Определение актуальных угроз информационной безопасности 16

6 Модель нарушителя информационной безопасности организации 19

7 Методы и средства обеспечения информационной безопасности 22

7.1 Система охранно-пожарной сигнализации 22

7.2 Система видеонаблюдения 25

7.3 Система контроля и управления доступом 28

7.4 Защита выделенного помещения 28

8 Реализация политики безопасности с использованием выбранных средств защиты 30

8.1 Система охранно-пожарной сигнализации 30

8.2 Система видеонаблюдения 35

8.3 Система контроля и управления доступом 38

8.4 Система защиты специального помещения 39

9 Организационные мероприятия по обеспечению информационной безопасности 40

10 Оценка стоимости реализации системы 43

Заключение 45

Список использованных источников 46

Приложение А Техническое задание на построение системы ИТЗ 48

Введение

В условиях постоянно развивающихся технологий и усиления цифровизации множества процессов вопрос защиты информации от нарушителей становится как никогда актуальным.

Современные предприятия функционируют в условиях высокой конкурентной среды и быстроменяющихся технологических реалий, что требует от них не только эффективного управления ресурсами, но и обеспечения безопасности своих операций. Инженерно-техническая защита информации (ИТЗИ) становится одним из ключевых инструментов для минимизации рисков, связанных с воздействием внешних и внутренних угроз. Построение системы ИТЗИ позволяет создать многослойную архитектуру, способную предотвратить или смягчить последствия несанкционированного доступа, кражи интеллектуальной собственности, а также различных видов саботажа изнутри организации.

Неправильное построение системы ИТЗИ может привести не только к финансовым потерям, но и к потере репутации, что в конечном итоге будет негативно сказываться на конкурентной способности предприятия. Таким образом, построение эффективной инженерно-технической защиты требует системного подхода, включающего анализ потенциальных угроз, оценку уязвимостей и внедрение современных инженерных решений.

Целью данной курсовой работы является разработка рекомендаций по построению системы инженерно-технической защиты для организации ООО «Мфитнес» с учетом его специфики и потребностей. В процессе исследования будут рассмотрены основные элементы ИТЗИ, проанализированы существующие угрозы и выработаны предложения по их минимизации.

1 Назначение и цели построения системы

Инженерно-техническая защита представляет собой комплекс инженерных и технических мероприятий, направленных на обеспечение защиты информационных ресурсов предприятия, защиты от несанкционированного проникновения, чрезвычайных ситуаций и других противоправных действий. Соответственно, основным назначением системы ИТЗИ является создание обширной системы предотвращения неконтролируемой утечки информации за пределы организации.

Цели построения комплекса инженерно-технической защиты:

– охрана предприятия, наблюдение за территорией и помещениями, осуществление контролируемого доступа в здание;

– выявление каналов утечки информации и их нейтрализация;

– обеспечение безопасности информации;

– минимизация рисков;

– защита секретных данных.

ИТЗИ можно разделить на следующие виды:

1. Физическая защита. К ней относятся охранно-пожарные системы, аварийное оповещение, системы контроля и управления доступом, а также различные извещатели;

2. Аппаратная защита. К ней относятся электронные и механические устройства, предназначенные для защиты информации и противодействия шпионажу;

3. Программная защита. К ней относятся различные системы защиты информации.

2 Описание предметной области

Объектом информатизации является компания ООО «Мфитнес», которая занимается продажами и установкой фитнес-оборудования и работает по всему региону, а также выполняет его ремонт и настройку.

Информационная система данной организации находится непосредственно в здании организации.

ООО «Мфитнес» располагается по адресу: Россия, Краснодарский край, г. Краснодар, ул. Коммунаров 270. Вход на территорию никак не защищен, доступ в помещение осуществляется через дверь с фасада здания.

Штат компании составляет 15 человек.

2.1 Описание объекта информатизации

В информационной системе организации циркулирует информация, составляющая персональные данные сотрудников и клиентов, а также сведения, составляющие коммерческую тайну. Эти сведения регулируют Федеральный закон №152-ФЗ «О персональных данных» [2], а также Федеральный закон №98-ФЗ «О коммерческой тайне».

К персональным данным, которые собирает организация относятся: ФИО, паспортные данные, ИНН, СНИЛС, дата рождения, юридический адрес, прописка.

К коммерческой тайне относятся сведения о закупленном оборудовании, его стоимости, количестве, источниках закупки, а также сведения о продажах и финансовом состоянии компании.

Никаких инженерно-технических мер безопасности на объекте информатизации не предусмотрено, что вызывает потенциальные угрозы информационной безопасности для организации.

Отсутствие таких мер, как системы контроля и управления доступом, видеонаблюдение, охранные сигнализации и физические барьеры, делает объект

уязвимым для различных видов угроз, включая несанкционированный доступ, вандализм и кражу оборудования. Более того, нехватка защиты может привести не только к утечке конфиденциальной информации, но и к поломке IT-инфраструктуры, что в свою очередь может повлечь существенные финансовые потери, вплоть до утраты данных, восстановление которых может быть сложным и затратным процессом.

Также отсутствие мер инженерно-технической безопасности может негативно сказаться на доверии со стороны клиентов, поскольку они могут опасаться за сохранность своих данных и других активов. Это может привести к снижению репутации организации и потере клиентов, что, в конечном итоге, скажется на ее конкурентоспособности на рынке.

Таким образом, наличие эффективных инженерно-технических мер безопасности является необходимым условием для обеспечения защиты информационных систем и стабильной работы объекта информатизации в целом.

2.2 Описание помещений объекта

Компания ООО «Мфитнес» расположена в офисном помещении на первом этаже жилого здания. План комнат организации с их площадями представлен на рисунке 1, а также на листе 1 в графической части.

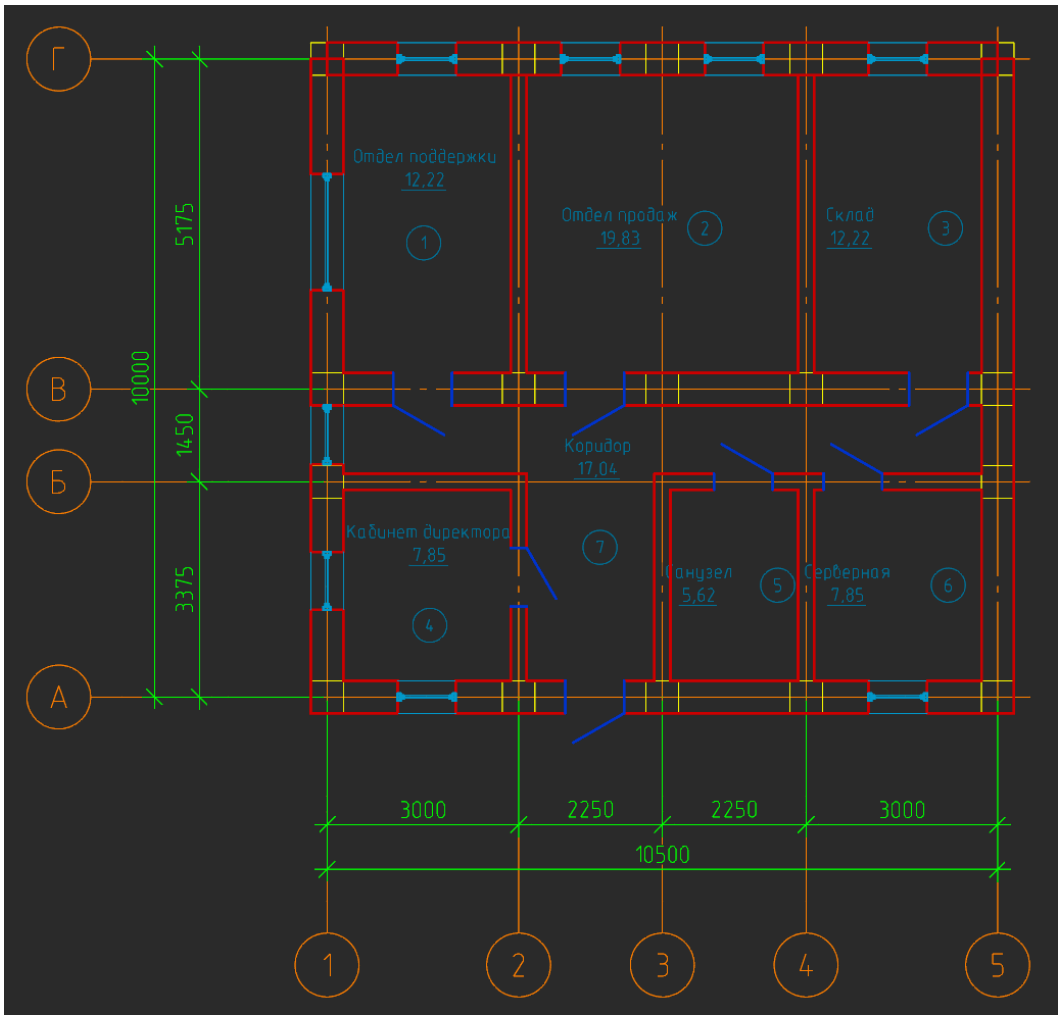

Рисунок 1 – План офиса

В офисе есть коридор, а также 6 помещений, которые он соединяет:

1. Отдел поддержки;
2. Отдел продаж;
3. Склад;
4. Кабинет директора;
5. Санузел;
6. Серверная.

Стены выполнены из кирпича. Толщина несущих стен составляет 510 мм (2 кирпича), ненесущих 250 мм (1 кирпич). Размеры оконных проемов: 920 мм и 1820 мм. Размеры дверей 920 мм. Высота потолков 3 м.

2.3 Обследование объекта информатизации

Утечка информации из организации может произойти по разным причинам и может привести к серьёзным последствиям. Также большие риски несет организация от потери имущества, которое хранится на ее территории. Таким образом, склад имеет площадь 12,2 м^2 и хранит в себе оборудование на ~1 миллион рублей. Также злоумышленники могут украсть прочую офисную технику, которая расположена на рабочих местах сотрудников.

Самая важная информация, которую обрабатывает организация – это персональные данные клиентов и сотрудников. Эти данные на бумажных носителях хранятся в кабинете директора и в помещении отдела продаж.

Для сохранения безопасности организации необходимо определить контролируемую зону, то есть территорию, на которой исключено неконтролируемое пребывание лиц, не имеющих допуска. Оптимальной границей контролируемой зоны будет периметр помещения организации и фасад здания.

Контрольные приборы для обнаружения сигналов с охранных и пожарных извещателей, а также видеорегистраторы, фиксирующие данные с камер видеонаблюдения можно расположить в серверной комнате.

В соответствии с РД 78.36.006-2005 «Рекомендации по выбору и применению технических средств охранно-пожарной сигнализации и средств инженерно-технической укрепленности для оборудования объектов» разделяются на две группы: А и Б. Для дальнейшего построения систем защиты информации необходимо определить категорию объекта. Опираясь на этот документ, организации ООО «Мфитнес» можно присвоить категорию Б1. К этой категории относятся объекты организаций различных форм собственности, преступные посягательства на которые могут привести к крупному и значительному материальному ущербу предприятию или собственнику и относятся к коммерческим объектам [9].

Местами возможного проникновения злоумышленников могут быть входные двери и окна помещения.

3 Концепция и политика информационной безопасности организации

Политика безопасности любой организации является неотъемлемой частью обеспечения информационной безопасности внутри ее. Она определят требования к автоматизированной системе с точки зрения защиты ее материальных и информационных ресурсов. Основная ее задача заключается в предотвращении инцидентов информационной безопасности [7].

Политика безопасности ООО «Мфитнес» разрабатывалась на основании следующих нормативно-правовых актов:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1];

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;

– Федеральный закон от 21 декабря 1994 года № 69-ФЗ «О пожарной безопасности»;

– ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом»;

– ГОСТ 12.1.004-91 «Система стандартов безопасности труда. Пожарная безопасность. Общие требования»;

– ГОСТ Р 52860-2007 «Технические средства физической защиты»;

– ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные».

Политика информационной безопасности также разграничивает доступ сотрудников к информационным ресурсам и физическим помещениям [3]. Таким образом, сотрудники из отдела поддержки не могут иметь полного доступа к персональным данным (ПД) клиентов компании, в отличии от директора или отдела продаж. В это же время сотрудники отдела продаж не имеют доступа к складу и

тому подобное. Была составлена матрица доступа, на которой обозначены должностные роли сотрудников и их права доступа – Таблица 1.

Таблица 1 – Матрица доступа сотрудников

Объект /субъект доступа	Директор	Отдел продаж	Отдел поддержки	Работник склада	Системный администратор
Склад	+	-	+	+	-
Серверная	+	-	-	-	+
Кабинет директора	+	-	-	-	-
ПД сотрудников	+	-	-	-	-
ПД клиентов	+	+	+-	-	-
Информация о закупах и продажах	+	+	+-	+	-
Данные об информационной системе	+	-	-	-	+

В результате разработки и применения матрицы доступа будут уменьшены риски, связанные с нарушением должностных инструкций сотрудников, а также усилится безопасность организации. Также ее применение упрощает управление правами сотрудников и помогает выявлять внутренних нарушителей. С расширением штата или усложнения должностных инструкций сотрудников следует актуализировать и дополнять матрицу доступа.

Также политика безопасности должна предусматривать инженерно-технические методы защиты информации, такие как:

- системы контроля и управления доступом;
- системы пожарной защиты;
- охранные системы;

– системы оповещения;

– системы видеонаблюдения.

Эти методы помогут создать многоуровневую систему защиты информации и повысят общий уровень безопасности в организации.

4 Постановка задачи

Задача курсовой работы состоит в построение комплекса инженерно-технической защиты для организации ООО «Мфитнес». Компания имеет в своем распоряжении офис, расположенный на первом этаже жилого здания. Периметр офиса изображен на листе 1 в графической части настоящей курсовой работы.

В соответствии с планами офиса перечень помещений организации указан в таблице 2.

Таблица 2 – Перечень помещений

Обозначение	Помещение	Площадь, $м^2$	Назначение	Кол-во работников
1	2	3	4	5
1	Отдел поддержки	12,2	В этом помещении находятся сотрудники, осуществляющие монтаж, ремонт и гарантийное обслуживание оборудования	4
2	Отдел продаж	19,8	Здесь находятся люди, отвечающие за процесс реализации продуктов и услуг организации	8
3	Склад	12,2	Хранение упаковочных материалов, некоторых товаров и ремонтного оборудования	1
4	Кабинет директора	7,9	Является рабочим пространством руководителя	1
5	Санузел	5,6	Личная гигиена сотрудников	-

Продолжение таблицы 2

1	2	3	4	5
6	Серверная	7,9	В этом помещении располагается сервер компании, а также работает системный администратор	1
7	Коридор	17,0	Связывает помещения	-

Суммарная площадь организации составляет 85,7 м^2. Число сотрудников, работающих в ООО «Мфитнес»: 15 человек.

Стоит отметить, что помещения серверной, кабинете директора и склада должны иметь повышенное внимание с точки зрения обеспечения безопасности, так как они являются помещениями специального назначения, то есть предназначены для размещения коммуникационного и технического оборудования, архива и товаров хранения. Выделенным помещением является кабинет директора.

4.1 Система инженерно-технической защиты

Информационная безопасность организации будет строится в основном с применением средств инженерно-технической защиты информации, т.к. благодаря им можно предотвращать большинство инцидентов безопасности в небольшой организации, как ООО «Мфитнес». Также ее применение будет не только самым эффективным, но и весьма незатратным.

Исходя из вышеперечисленных данных и чертежа офиса компании были определены основные направления по обеспечению защищенности информации. Таким образом, необходимо обеспечить создание нескольких систем по обеспечению инженерно-технической безопасности. Таких как:

– система пожарной сигнализации. Она должна обеспечить подачу светового и звукового сигналов о возникновении пожара на приемно-контрольный прибор, который необходимо установить в серверном помещении. Эту систему

можно реализовать с использованием различных противопожарных извещателей, например: дымовых, тепловых или универсальных еще необходимо обеспечить оповещение о возгорании и задымлении помещений и разработать план эвакуации;

– система охранной сигнализации. Она также должна обеспечить подачу сигнала на приемно-контрольный прибор, но уже в случае несанкционированного проникновения постороннего лица на территорию организации или при нарушении сотрудника своих прав доступа. Эта комплексная система может включать в себя: датчики разбития окна, открывания дверей, датчики объема и движения, экстренные кнопки, а также устройство оповещения;

– система видеонаблюдения должна считывать информацию с территории в радиусе своего действия. Эта система должна охватывать весь периметр контролируемой зоны организации для обеспечения постоянного наблюдения за происходящим. Данная система включает в себя камеры видеонаблюдения различных типов (купольные и цилиндрические, внутренние и внешние, аналоговые и цифровые) и видеорегистраторы – приборы, считывающие информацию с камер и записывающие ее на цифровые носители или облачное хранилище;

– система контроля и управления доступом (СКУД). Основная задача этой системы – это обеспечить контрольно-пропускной режим на территорию объекта. Существует множество способов реализации данной системы безопасности, начиная от турникетов, заканчивая дверьми, сканирующими ваши биометрические данные;

– система защиты помещений специального назначения. Как уже было сказано выше такие помещения должны иметь повышенную защиту, так как являются особо важными с точки зрения безопасности организации. Данную систему можно реализовать с использованием ранее перечисленных методов, таких как СКУД или система видеонаблюдения.

Данная функциональная система объекта информатизации позволит обеспечить достаточный контроль над безопасностью организации и поддерживать высокий уровень защищенности.

Доступ к рабочим местам предоставляется только после ознакомления и подписания сотрудником документа, регламентирующим технику безопасности и политику безопасности, согласно его должностным обязанностям.

5 Определение актуальных угроз информационной безопасности

Угрозы информационной безопасности представляют собой потенциальные события или действия, которые могут нанести вред информационным системам, данным и ресурсам организации. Эти угрозы могут быть вызваны различными факторами, включая человеческие ошибки, намеренные действия злоумышленников, технические сбои или природные катастрофы.

Для оценки потенциальных угроз информационной безопасности необходимо их классифицировать по следующим признакам:

– источники угроз. Внутренние или внешние;

– уровень воздействия угроз. Необходимо определить к каким негативным последствиям, таким как утечка конфиденциальной информации, финансовые потери, повреждение репутации, утрата оперативной эффективности и юридические последствия, может привести реализация угрозы;

– оценка угрозы. Для эффективного регулирования информационной безопасности важно оценить уровень риска тех или иных угроз, это поможет определить вероятные сценарии развития событий и возможные последствия;

– способ защиты. На основании оценки угроз необходимо разработать мери по снижению рисков инцидентов безопасности.

Определение угроз информационной безопасности является ключевым элементом при управлении безопасностью и снижении рисков, позволяет использовать наиболее эффективные меры для защиты объекта.

Для определения актуальных угроз организации следует опираться на законодательство Российской Федерации. Анализ актуальных угроз выполняется в соответствии со следующими нормативными документами: Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и Методикой оценки угроз информационной безопасности (далее Методика), утвержденной Приказом ФСТЭК России от 5 февраля 2021 года [5].

Согласно статье 19 Федерального закона № 152-ФЗ «О персональных данных», организация при обработке персональных данных обязана применять

необходимые меры для защиты персональных данных от несанкционированного доступа, уничтожения, изменения, копирования и так далее. Обеспечение безопасности персональных данных достигается, в первую очередь, определением угроз безопасности при их обработке в информационных системах.

Исходя из пункта 5.2 «Оценка способов реализации угроз безопасности информации» настоящей Методики, общий перечень угроз информационной безопасности содержится в банке угроз безопасности информации на сайте ФСТЭК России (bdu.fstec.ru). Из этого перечня были выделены следующие актуальные угрозы, реализация (возникновение) которых может привести к нарушению безопасности для ООО «Мфитнес» и представлены в таблице 3.

Таблица 3 – Актуальные угрозы

Вид угрозы	Источник угрозы	Вероятность реализации	Показатель опасности
1	2	3	4
Разглашение персональных данных	Внутренние нарушители	Низкая	Высокая
Утечка информации, составляющей коммерческую тайну	Внутренние и внешние нарушители	Средняя	Средний
Несанкционированный доступ	Внутренние нарушители	Высокая	Высокий
Разглашение конфиденциальной информации	Внутренние нарушители	Низкая	Средний

Продолжение таблицы 3

1	2	3	4
Вандализм	Внешние нарушители	Средняя	Средний
Хищение имущества	Внутренние и внешние нарушители	Средняя	Высокий

На основе данных, представленных в таблице 3, можно сделать вывод о том, что в первую очередь необходимо защититься от угроз высокого уровня, так как они представляют наивысшую опасность для организации и ведут к негативным последствиям.

6 Модель нарушителя информационной безопасности организации

Модель нарушителя была разработана, опираясь на «Рекомендуемую структурную модель угроз безопасности информации», представленной в Методике оценки угроз безопасности информации. Любых нарушителей любой организации можно классифицировать, как внешних и внутренних.

К внешним нарушителям относятся лица, не имеющих прав доступа во внутрь контролируемой зоны и не имеющих доступа к информационной системе на момент начала реализации угрозы.

Под внутренним нарушителем понимают лицо, имеющее доступ к контролируемой зоне или находящегося внутри информационной системы организации в момент начала реализации угрозы. К таким нарушителям можно отнести и инсайдеров несмотря на то, что они выполняют инструкции лиц, находящихся за пределами организации.

Опираясь на методический документ, утвержденный Приказом ФСТЭК России, от 5 февраля 2021 года «Методика оценки угроз безопасности информации», можно выделить следующие группы нарушителей, актуальные для ООО «Мфитнес», они представлены в таблице 4 и являются моделью нарушителя.

Таблица 4 – Модель нарушителя

Виды нарушителя	Категория нарушителя	Цели реализации угроз
1	2	3
Преступные группы	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации

Продолжение таблицы 4

1	2	3
Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
Отдельные физические лица	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации
Лица, обеспечивающие поставку оборудования	Внешний	Получение финансовой или иной материальной выгоды
Бывшие работники	Внешний	Получение финансовой или иной материальной выгоды. Месть
Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные действия
Лица, обеспечивающие функционирование систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные действия
Авторизированные пользователи	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации. Месть. Непреднамеренные действия

Указанные цели реализации угроз являются абстрактными и приблизительными и могут конкретизироваться от случая к случаю.

Также стоит отметить, что нарушители одних групп могут для повышения своих возможностей вступать в сговор с нарушителями других групп. В случае

принятия таких предложений необходимо объединять их цели и уровни возможностей.

Основываясь на модели нарушителя, можно дополнить политику безопасности, создав более эффективные политики и процедуры для защиты активов организации.

7 Методы и средства обеспечения информационной безопасности

7.1 Система охранно-пожарной сигнализации

Технические средства охранно-пожарной сигнализации – это устройства, предназначенные для фиксирования на охраняемом объекте фактов возгорания и/или несанкционированного проникновения человека на территорию предприятия и передачи соответствующей информации на приемно-контрольный прибор.

При построении системы охранно-пожарной сигнализации используется несколько типов устройств [8]:

а) извещатель – это устройство, предназначенное для обнаружения изменений в окружающей среде, таких как дым, огонь, газ или движение. Он выполняет следующие функции:

1) выявляет опасные ситуации (например, пожар или утечку газа);
2) передает сигнал тревоги на центральный контрольный прибор.

б) оповещатель – это устройство, которое информирует людей и чрезвычайной ситуации. Он выполняет следующие функции:

1) издает звуковые, световые или речевые сигналы для предупреждения о возникновении опасности;
2) уведомляет людей о необходимости покинуть помещение определенным образом или принят соответствующие меры безопасности.

в) приемно-контрольный прибор – это устройств, которое принимает сигналы от извещателей и управляет работой системы оповещения. Он выполняет следующие функции:

1) сбор и обработка сигналов тревоги от различных извещателей;
2) отображение состояния системы и информации о поданных тревогах;
3) управление работой оповещателей в соответствии с полученными сигналами от извещателей.

г) прибор управления – это устройство, отвечающие за управление всеми компонентами системы безопасности. Он выполняет следующие функции:

1) настройка параметров работы извещателей и оповещателей;

2) формирование о отправка команд на исполнительные устройства охраны, например блокировка системы вентиляции, запуск системы автоматического пожаротушения и так далее.

Согласно ГОСТ 12.1.004-91 «Пожарная безопасность. Общие требования» при высоте потолка 3 метра извещатели имеют радиус покрытия в 9 метров. Таким образом, на 7 помещений необходимо минимум 7 извещателей, так как все помещения полностью покрываются одним извещателем и еще дополнительный извещатель для коридора из-за сложной формы помещения.

Для охраны здания будут использоваться приборы контроля разбития окна, на 9 окон соответственно 9 штук, контроля открытия дверей: 2 штуки.

Исходя из вышесказанного необходимо использовать приемно-контрольный прибор пожарной сигнализации необходимо использовать как минимум на 16 извещателей, чтобы оставался запас на охранную сигнализацию.

На каждое помещение будет использовано по одной линии приемно-контрольного прибора. Одна линия на пожарную сигнализацию и вторая на охранную. Таким образом, необходимо использовать извещатель как минимум на 7 линий для пожарной сигнализации.

Соответственно, под описание подходит ППК «Гранит-16» и «ВЭРС-ПК 24П». Исходя из сравнения характеристик и отзывов на оба прибора, стало понятно, что они имеют примерно одинаковый функционал и возможности, следовательно целесообразнее использовать более дешевый, а именно «Гранит-16».

Для определения возгорания в помещении будут использованы дымовые оптико-электронные противопожарные извещатели «ИП 212-45», так как эта модель является самой эффективной и оптимальной по соотношению цена-качество. Этот извещатель также является проводным и питается по двухжильному кабелю. Извещатель имеет помехоустойчивость по ГОСТ Р 53325 и способ защиты от

поражения током 3 класса, а также степень защиты IP 30, а срок службы не менее 10 лет. Он совместим с приборами Гранит.

Также необходимо использовать ручные пожарные извещатели. «ИПР-55К» подойдет для этой задачи.

В качестве датчика разбития стекла будет использован извещатель охранный поверхностный звуковой «Астра-С», так как этот датчик является одним из самых популярных. Его технические характеристики в сравнении с извещателем «Стекло-3» представлены в таблице 5.

Таблица 5 – Сравнение характеристик звуковых извещателей

Характеристика	Астра-С	Стекло-3
Класс защиты	IP30	IP30
Тип крепления	В оконный и дверной проем, на стену, на потолок	На стену, на потолок
Регулировка чувствительности	Есть	Есть
Тампер вскрытия корпуса	Есть	Есть
Ток потребления, мА	12	22
Напряжение, В	8-15	9-17
Стоимость, руб	839	862

Извещатели имеют похожие характеристики, но выделяются электропотребление и стоимость, что сокращает единоразовые, и, хоть и не существенно, но сокращает долговременные затраты.

Для обеспечения защиты открытия дверей будет использован магнитоконтактный извещатель «ИО 102-2», так как он является самым популярным и надежным среди подобных датчиков.

В качестве охранно-пожарного оповещателя будет использован речевой оповещатель «СОНАТА-3», и также будут использованы стандартные пожарные указатели в виде табличек на стены.

По правилам пожарной безопасности помещение классифицируется как класс Е – воспламенение электрооборудования. Это значит, что огнетушители должны располагаться на расстоянии до 70 метров друг от друга. Для офисного помещения подойдет порошковый огнетушитель ОП-4. Их необходимо установить в коридоре в количестве двух штук, для обеспечения максимального покрытия.

В качестве резервного питания необходимо использовать специальный источник бесперебойного питания. Для таких целей существуют специализированные устройства для охранно-пожарных извещателей, такой линейкой является СКАТ. Для питания 16 шлейфов ППК подойдет ИБП СКАТ-1200У.

7.2 Система видеонаблюдения

Система видеонаблюдения – совокупность программных и технических средств для записи и хранения видеоданных и осуществления информационного обмена между собой.

Эта система включает в себя следующие устройства:

- видеокамеры;
- видеорегистратор;
- монитор для вывода изображения;
- жесткие диски для сохранения видео;
- инфраструктура для передачи сигналов (роутер или кабели).

Изначально в организации не было расположено системы видеонаблюдения. Это ведет к появлению угроз информационной безопасности. Для предотвращения реализации этих угроз необходимо обеспечить создание системы видеонаблюдения

для обеспечения полного обзора всех помещений организации и периметра контролируемой зоны.

Для обеспечения надежной системы видеонаблюдения необходимо использовать различные типы камер:

– купольные в виде полусферы с плоским основанием. Обладают антивандальными свойствами и подходят для установки внутри помещений на потолки и стены;

– цилиндрические. Устанавливаются на улице – на столбах, заборах, стенах зданий.

Таким образом, в зависимости от места установки, необходимо использовать различные типы видеокамер.

В качестве прибора наблюдения внутри помещения выбор стоял между продуктами компаний HiWatch и Dahua. В качестве сравнительных экземпляров были выбраны видеокамеры «HiWatch DS-I102» и «Dahua DH-IPC-HDW1230T1P-0360B-S5». Сравнительная характеристика этих камер представлена в таблице 6.

Таблица 6 – Сравнительная характеристика IP-видеокамер

Характеристика	HiWatch DS-I102	Dahua DH-IPC-HDW1230T1P-0360B-S5
Питание	12 DC/PoE	12 DC/PoE
Кодеки сжатия	H.265/H.265+/H.264/ H.264+/MPEG4	H.265+/H.265/H.264+/H.264/ H.264B/H.264H/MJPEG
Объектив, мм	2.8	2.8
Разрешение	1920x1080	1920x1080
Класс защиты	IP67	IP67
Стоимость, руб	4290	5592

Исходя из сравнительной характеристики можно сделать вывод о том, что видеокамеры являются аналогами друг друга от разных производителей, поэтому

целесообразнее отдать предпочтение более бюджетному решению, то есть «HiWatch DS-I202».

В качестве камеры наружного наблюдение следует также использовать продукцию этой компании для общей совместимости с видеорегистратором. Таким образом, выбор стоит между двумя IP-камерами: модель DS-I200 и IPC-B020. Исходя из технических характеристик обеих камер была выбрана первая модель, так как она имеет ряд преимуществ: питание с помощью технологии PoE, больший угол обзора и лучшее качество изображения.

Для записи видеоматериала на физические носители необходимо использовать видеорегистратор. Так как выбранные камеры работают по протоколу IP и имеют технологию PoE, следует использовать видеорегистратор с поддержкой этих функций. Следовательно, из линейки HiWatch самым лучшим решением будет продукт «HiWatch DS-N208P9(C)». Он обладает поддержкой вышеперечисленных технологий и поддерживает жесткий диск объемом до 6 Тб. К себе он способен подключить до 8 IP-камер.

Воспользовавшись калькулятором объема жесткого диска на официальном сайте производителя видеокамер, представленном на рисунке 2, можно сделать вывод о том, что для записи видеоматериала на диски необходим объем минимум 12 Тб.

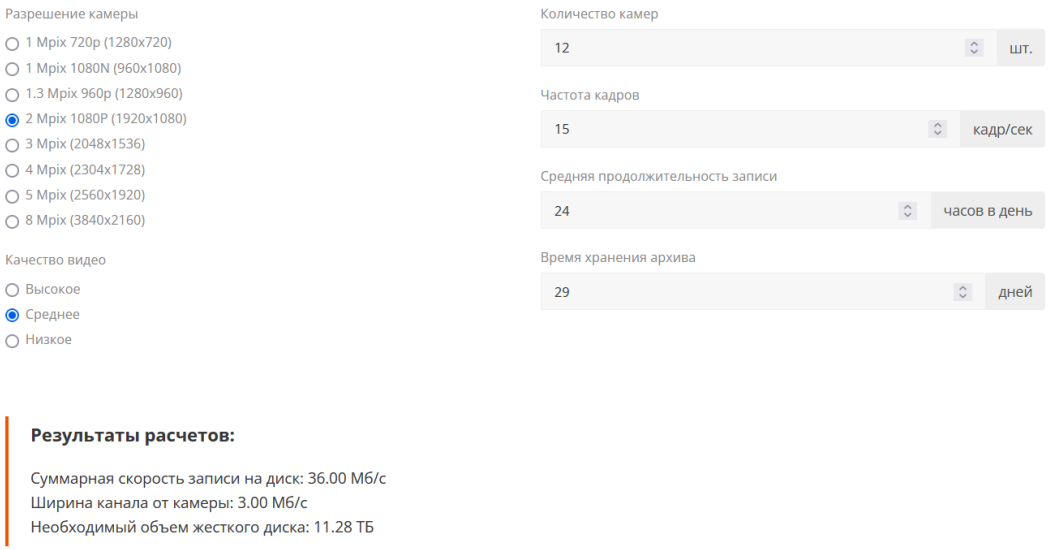

Рисунок 2 – Расчет объема накопителей

В качестве хранилища данных будут использоваться жесткие диски Seagate SkyHawk объемом 6 Тб, в количестве двух штук, предназначенные специально для систем видеонаблюдения: сводят к минимум количество потерянных кадров и время простоя, при этом они рассчитаны на рабочее время нагрузки в три раза большее по сравнению с дисками для настольных компьютеров.

Для вывода видеоинформации будет использоваться бюджетный монитор от фирмы DEXP модель DF24N2 на 24 дюйма.

7.3 Система контроля и управления доступом

Система контроля и управления доступом (СКУД) — это комплекс технических средств и программных решений, предназначенных для управления доступом в определенные помещения или территории. Основная задача СКУД — обеспечить безопасность, защиту имущества и контроль над перемещением людей.

На объекте необходимо обеспечить хотя бы базовый контроль доступом. В этих целях можно использовать считыватель смарт-карт для входа во внутрь контролируемой зоны. Для этого можно использовать продукт «ProxWay PW-mini Multi BLE v2 B», так как он поддерживает большинство стандартов умных карт и является лидером продаж. Он будет установлен на вход.

Для выхода из здания будет использоваться кнопка, при ее нажатии магнитная дверь будет открываться. Оба этих средства являются автономными и не требуют специального приемного прибора.

7.4 Защита выделенного помещения

В качестве выделенного помещения выступает кабинет директора организации. Именно в этом помещении ведутся конфиденциальные переговоры.

Для защиты этого помещения необходимо избавиться или минимизировать возможность утечки информации по различным техническим каналам утечки информации [10]:

– акустические. Этот канал связан с передачей звуковых сигналов и возникновением колебаний в различных средах за счет звуковых волн;

– визуально-оптические. Перехват информации происходит визуально;

– материально-вещественные. В этом случае источниками информации являются материальные объекты;

– радиоэлектронные. В этих каналах средой переноса сигналов является электрический ток или различные поля.

Для предотвращения утечки по акустическому каналу необходимо использовать специальные технические средства [5]. В качестве такого средства можно использовать генератор шума, такой как «ЛГШ-304». Он имеет сертификат ФСТЭК России по 2 классу защиты, значит подходит для помещения, в котором обрабатывается информация, составляющая государственную тайну. Помещение, в котором он устанавливается имеет меньший класс защищенности, значит, данное средство подходит для использования.

8 Реализация политики безопасности с использованием выбранных средств защиты

Необходимо реализовать составленную политику безопасности с помощью использования выбранных средств защиты информации, согласно поставленным задачам обеспечения безопасности.

8.1 Система охранно-пожарной сигнализации

Разработанный план охранно-пожарной сигнализации, разработанный в соответствии с регламентом политики безопасности и ГОСТами пожарной безопасности представлен на листе 2 в графической части настоящей курсовой работы.

План эвакуации при пожаре представлен на листе 5 в графической части курсовой работы.

Приемно-контрольный прибор «Гранит-16» представлен на рисунке 3, и его установка выполнена согласно изображению на рисунке 4.

Рисунок 3 – Приемно-контрольный прибор «Гранит-16»

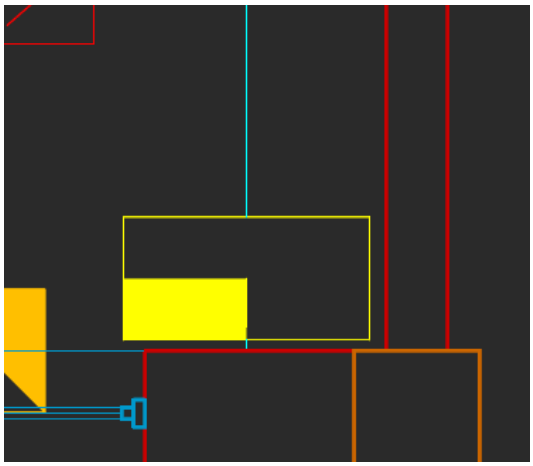

Рисунок 4 – Расположение ППК «Гранит-16»

Пожарный извещатель «ИП 212-45» представлен на рисунке 5, и его установка выполнена согласно изображению на рисунке 6.

Рисунок 5 – Пожарный извещатель «ИП 212-45»

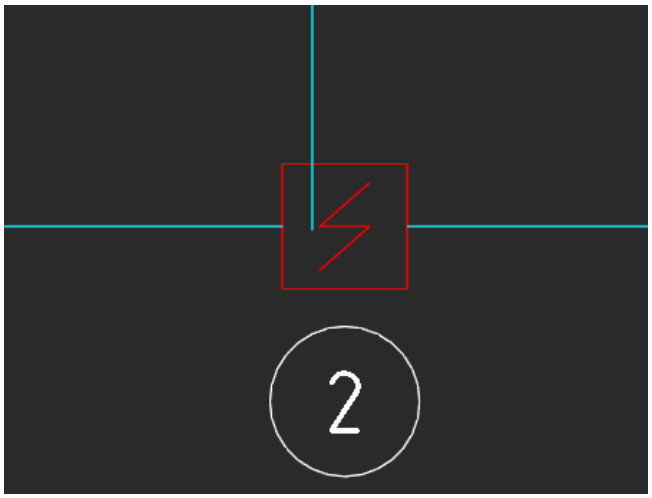

Рисунок 6 – Расположение «ИП 212-45» в отделе продаж

Ручной пожарный извещатель «ИПР-55К» представлен на рисунке 7, и его установка выполнена согласно изображению на рисунке 8.

Рисунок 7 – Ручной пожарный извещатель «ИПР-55К»

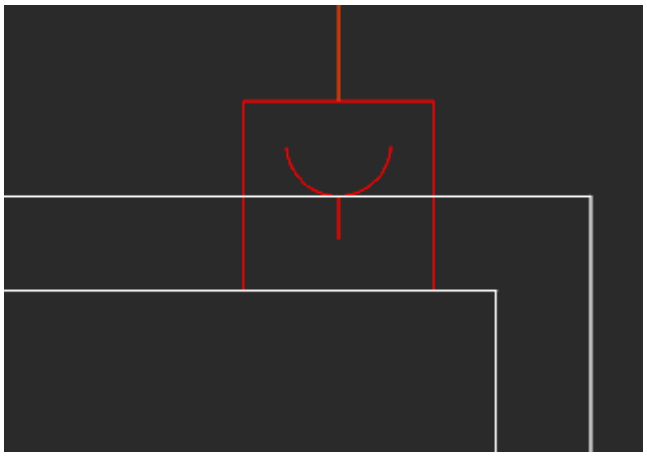

Рисунок 8 – Расположение «ИПР-55К» на примере коридора

Извещатель разбития стекла «Астра-С» представлен на рисунке 9, и его установка выполнена согласно изображению на рисунке 10.

Рисунок 9 – Извещатель разбития стекла «Астра-С»

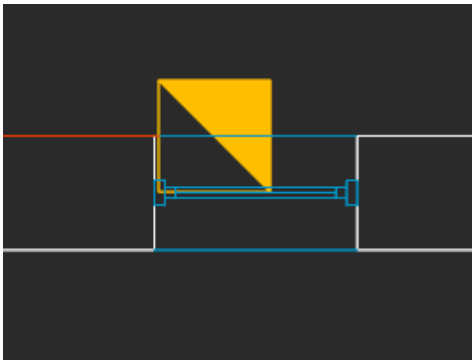

Рисунок 10 – Расположение «Астра-С» на примере серверной

Датчик открытия двери – магнитоконтактный извещатель «ИО 102-2» представлен на рисунке 11, и его установка выполнена согласно изображению на рисунке 12.

Рисунок 11 – Извещатель «ИО 102-2»

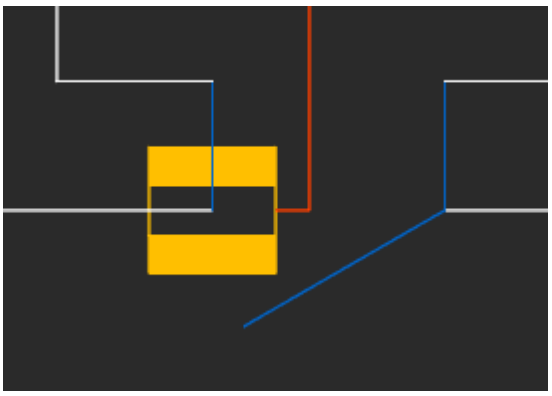

Рисунок 12 – Расположение датчика «ИО 102-2» на примере входной двери

Оповещатель охранно-пожарный речевой «СОНАТА-3» представлен на рисунке 13, и его установка выполнена согласно изображению на рисунке 14.

Рисунок 13 – Оповещатель «СОНАТА-3»

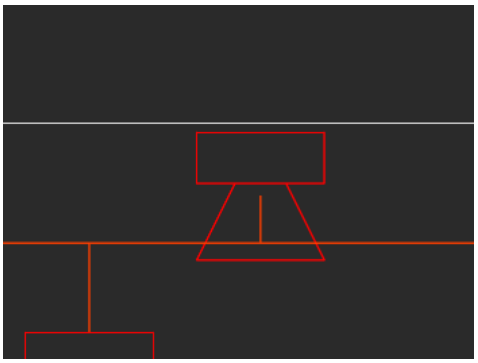

Рисунок 14 – Расположение оповещателя «СОНАТА-3» в коридоре

Установка извещателей была выполнена согласно стандартам пожарной и охранной безопасности. На схеме 4 в графической части изображен план пожарной эвакуации.

8.2 Система видеонаблюдения

Внутренние видеокамеры «HiWatch DS-I102» представлены на рисунке 15, и их установка выполнена согласно изображению на рисунке 16.

Рисунок 15 – IP-камера «HiWatch DS-I102»

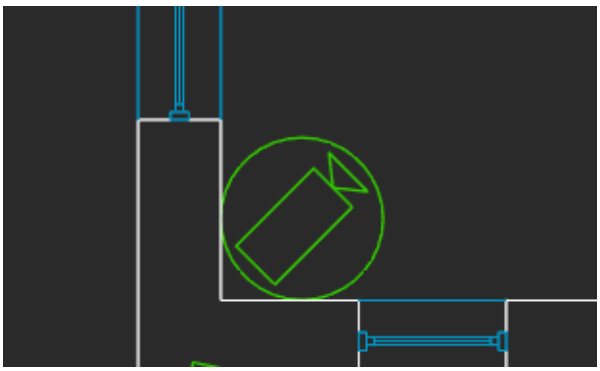

Рисунок 16 – Расположение внутренних камер в кабинете директора

Внешние камеры «HiWatch DS-I200» представлены на рисунке 17, и их установка выполнена согласно изображению на рисунке 18.

Рисунок 17 – IP-камера «HiWatch DS-I200»

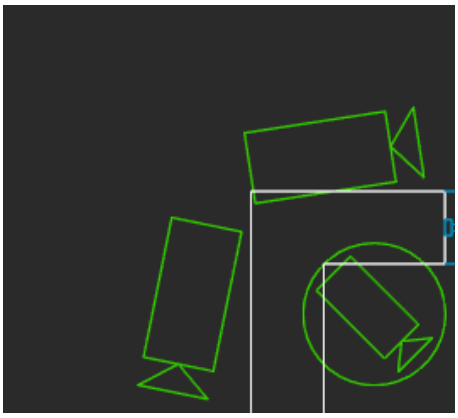

Рисунок 18 – Расположение внешних камер на углу здания

Видеорегистратор «HiWatch DS-N208P9(C)» представлен на рисунке 19, и его установка выполнена согласно изображению на рисунке 20.

Рисунок 19 – Видеорегистратор «HiWatch DS-N208P9(C)»

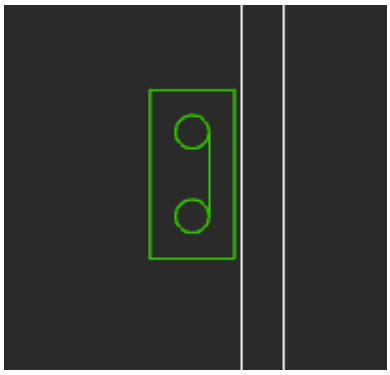

Рисунок 20 – Расположение видеорегистратора в серверной

Жесткий диск «Seagate SkyHawk 6 ТВ» представлен на рисунке 21.

Рисунок 21 – Жесткий диск «Seagate SkyHawk 6 ТВ»

Монитор «DEXP DF24N2» представлен на рисунке 22.

Рисунок 22 – Монитор «DEXP DF24N2»

План системы видеонаблюдения представлен на листе 3 в графической части настоящей курсовой работы.

8.3 Система контроля и управления доступом

Считыватель «ProxWay PW-mini Multi BLE v2 B» представлен на рисунке 23, и его установка вместе с кнопкой выполнена согласно изображению на рисунке 24.

Рисунок 23 – Считыватель «ProxWay PW-mini Multi BLE v2 B»

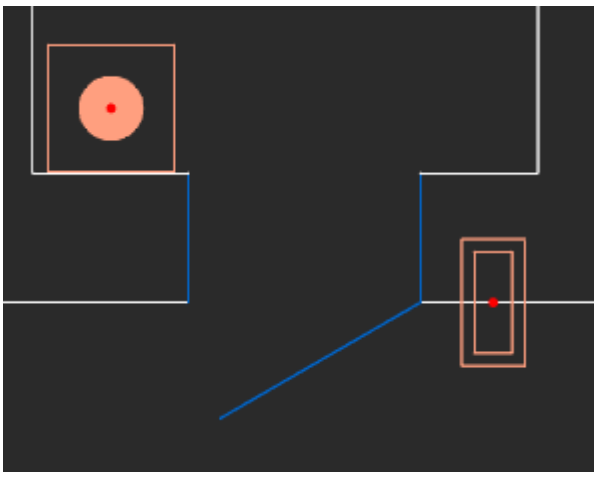

Рисунок 24 – Расположение считывателя и кнопки у входа

План системы видеонаблюдения представлен на листе 3 в графической части курсовой работы.

8.4 Система защиты специального помещения

Генератор шума «ЛГШ-304» представлен на рисунке 25.

Рисунок 25 – Генератор шума «ЛГШ-304»

Источник резервного питания «СКАТ-1200У» представлен на рисунке 26.

Рисунок 26 – Источник резервного питания «СКАТ-1200У»

Все системы расположены согласно стандартам и нормативным актам и выполняют поставленную задачу согласно созданной политики безопасности организации ООО «Мфитнес».

9 Организационные мероприятия по обеспечению информационной безопасности

Организационные мероприятия по обеспечению защиты информации – это набор процедур, политик, практик и правил, которые внедряются в организации для обеспечения безопасности информации. Организационные меры предусматривают установку временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации [6]. Эти меры помогают защитить информационные системы, сети и ресурсы от внутренних и внешних угроз, таких как несанкционированный доступ, утечка данных и прочие.

Организационные меры должны включать актуализацию политики безопасности, регулярное проведение аудита и оценку безопасности информационных сетей, ресурсов и помещения, а также обучение персонала.

Алгоритм актуализации политики безопасности должен состоять из трех этапов:

– этап 1. Провести пересмотр действующей политики информационной безопасности в установленный срок. Для начала процесса рекомендуется издать распорядительный документ. Пересмотр должен осуществлять либо разработчик политики, либо назначенное ответственное лицо. Результаты работы на этом этапе могут быть оформлены в виде отчета или заключения, включая конкретные предложения по всем необходимым изменениям;

– этап 2. Систематизировать и расставить приоритеты для всех предложенных изменений. Эту задачу может выполнить как сотрудник, указанный на Этапе 1, так и специалисты, отвечающие за соответствующие процессы или области;

– этап 3. Согласовать все необходимые коррективы, внести изменения в существующий документ, а затем утвердить обновленную политику информационной безопасности, аннулировав прежнюю версию документа.

Аудит информационной безопасности – это процесс оценки системы защиты информации на предмет соответствия стандартам и требованиям безопасности, а также выявление уязвимостей и возможных угроз информационной безопасности.

Основной целью аудита является выявление уязвимостей в системе защиты информации и предотвращение возможных угроз безопасности. Кроме того, аудит также позволяет определить эффективность системы защиты, а также позволяет проверить соответствие системы законодательству и стандартам безопасности.

Аудит информационной безопасности организации выполняется раз в месяц системным администратором компании. Также алгоритм аудита включает в себя проверку работоспособности системы видеонаблюдения.

Обучение персонала информационной безопасности должно включать в себя следующие меры:

– противодействие социальной инженерии. Сотрудников следует научить различать методы, используемые злоумышленниками для манипуляции и получения конфиденциальной информации;

– противодействие фишингу. Обучение идентификации фишинг-атак, использование технологии фильтрации, предоставление инструкции по действиям в случае получения фишингового сообщения, например, на электронную почту;

– правила работы с конфиденциальной информацией. Необходимо обучить правильному хранению данных, разделение полномочий, обучение правильной обработке данных (правила передачи, хранения и уничтожения конфиденциальной информации);

– правила использования паролей. Важно регулярно менять пароли на рабочих местах сотрудников и приучить запоминать пароли, а не записывать их, так как злоумышленник может обнаружить запись и получить доступ. Также необходимо создать парольную политику безопасности;

– правила поведения в интернете. Ответственное использование ресурсов, избегание подозрительных сайтов, защита личной информации;

– правила проведения секретных переговоров. При проведении переговоров нужно выключать все электронные устройства в комнате, где ведется конфиденциальный разговор;

– повышение осведомленности сотрудников об угрозах ИБ. Проведение регулярных тренингов, информирование сотрудников об инцидентах ИБ, разработка и распространение руководств и памяток по информационной безопасности в организации;

– обучение использования технического оборудования. Необходимо обучить персонал использовать установленные технические компоненты системы защиты информации.

10 Оценка стоимости реализации системы

Итоговая оценка стоимости реализации системы инженерно-технической защиты организации ООО «Мфитнес» представлена в таблице 7.

Таблица 7 – Оценка стоимости

Система	Компонент	Количество, шт	Стоимость, ₽
Охранно-пожарная сигнализация	Прибор приемно-контрольный	2	12210
	Световые указатели	9	800
	Дымовой извещатель	8	725
	Ручной извещатель	1	273
	Оповещатель	2	480
	Датчик разбития стекла	7	938
	Магнитоконтактный извещатель	2	130
	Огнетушитель	7	1289
Видеонаблюдение	Внутренняя камера	9	4290
	Внешняя камера	3	5550
	Видеорегистратор	2	11399
	Жесткий диск	2	14799
	Монитор	1	8399
СКУД	Считыватель карт	1	10380
	Кнопка	1	1000
Защита выделенного помещения	Генератор шума	1	25220
	ИБП	1	16020
		Итого:	223 177

Исходя из данных, представленных в таблице 7, можно сделать вывод о том, что разработанная система инженерно-технической защиты обладает стоимостью в двести двадцать три тысячи сто семьдесят семь рублей, без учета стоимости монтирования, настройки и сопровождения.

Заключение

Результатом выполнения курсового проекта является разработанная система инженерно-технической защиты компании «Мфитнес».

В ходе работы были проанализированы актуальные угрозы, с которыми может столкнуться организация, а также рассмотрены ключевые элементы эффективной системы ИТЗИ. Предложенные рекомендации по внедрению инженерно-технических средств защиты способны минимизировать риски, связанные с несанкционированным доступом и проникновением.

Разработанная система инженерно-технической защиты включает в себя следующие меры по обеспечению безопасности в организации:

- система охранно-пожарной сигнализации;
- система видеонаблюдения;
- система контроля и управления доступом;
- система защиты специального помещения.

Реализованная система защиты информации позволяет эффективно обеспечить защиту организации от существующих угроз. В то же время необходимо обеспечить и следить за выполнением организационно-технических мер, чтобы разработанная система оставалась такой же эффективной, как и задумывалась.

Список использованных источников

1. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ: редакция от 12.12.2023: принят Государственной Думой 8 июля 2006 года. – Текст: электронный // СПС «Гарант» [сайт] URL: https://ivo.garant.ru/#/document/12148555/ (дата обращения: 05.12.2024).

2. Российская Федерация. Законы. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ: редакция от 08.05.2023: принят Государственной Думой 8 июля 2006 года. – Текст: электронный // СПС «Гарант» [сайт] URL: https://ivo.garant.ru/#/document/12148567/ (дата обращения: 05.12.2024).

3. Российская Федерация. Постановления. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119. – Текст: электронный // СПС «Гарант» [сайт] URL: https://ivo.garant.ru/#/document/70252506/ (дата обращения: 05.12.2024).

4. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Методика оценки угроз безопасности информации: Методический документ от 5 февраля 2021 г: редакция от 06.12.2022. – Текст: электронный // СПС «Консультант Плюс» [сайт] URL: https://www.consultant.ru/document/cons_doc_LAW_378330/ (дата обращения: 05.12.2024).

5. Solar: [сайт]. – Текст. Изображение: электронные. – URL: https://rt-solar.ru/products/solar_dozor/blog/2085/ (дата обращения: 05.12.2024).

6. StaffCop [сайт]. – Текст. Изображение: электронные. – URL: https://www.staffcop.ru/blog/organizatsionnye-mery-zashchity-informatsii/ (дата обращения: 05.12.2024).

7. FalconOgraze [сайт]. – Текст. Изображение: электронные. – URL: https://falcongaze.com/ru/pressroom/publications/politika-informacionnoj- bezopasnosti /politika-informacionnoj-bezopasnosti/ (дата обращения: 05.12.2024).

8. SearchInform [сайт]. – Текст. Изображение: электронные. – URL: https://www.unitest.ru/about/publication/sredstva-pozharnoy-signalizatsiy.html (дата обращения: 05.12.2024).

9. Secutec [сайт]. – Текст. Изображение: электронные. – URL: http://secuteck.ru/articles2/kompleks_sys_sec/kategorirovanie_obiektov/kategorirovanie_obiektov_1.html (дата обращения: 05.12.2024).

10. AntiMalware [сайт]. – Текст. Изображение: электронные. – URL: https://www.anti-malware.ru/ practice/ methods/ information- from- leakage- through-acoustic -channels-protection (дата обращения: 05.12.2024).