

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

**«Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 111»**

Выполнил:

Григорьев А.П., студент
группы N34511



(подпись)

Проверил преподаватель:

Попов И.Ю., к.т.н., доцент
ФБИТ



(подпись)

Отметка о выполнении:



Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Григорьев А.П.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 111

Задание Проанализировать возможные каналы утечки информации в помещении, разработать меры пассивной и активной защиты информации, рассчитать их стоимость.

Краткие методические указания

Содержание пояснительной записки

Курсовая работа содержит введение, теоретическую часть, анализ защищаемых помещений, выбор средств защиты информации, расчет стоимости мер защиты, заключение, список использованных источников.

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Григорьев А.П.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 111

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу	27.10.2023	27.10.2023	
2	Анализ материалов	24.11.2023	24.11.2023	
3	Написание курсовой работы	17.12.2023	17.12.2023	
4	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель _____

(Подпись, дата)

Студент _____

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент Григорьев А.П.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 111

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

2. Характер работы

☐ Расчет

☒ Конструирование

☐ Моделирование

☐ Другое: Отчет

3. Содержание работы

Курсовая работы включает разделы: введение, организационная структура предприятия, обоснование защиты информации, план помещения, анализ рынка, расчет стоимости мер защиты, заключение, список использованных источников.

4. Выводы

В результате выполнения работы был проведен анализ каналов утечки информации в помещениях предприятия, разработаны меры пассивной и активной защиты информации, рассчитана стоимость предложенных мер.

Руководитель _____

(Подпись, дата)

Студент 

(Подпись, дата)

«17» декабря 2023 г

СОДЕРЖАНИЕ

Введение	6
1 Организационная структура предприятия	7
2 Обоснование защиты информации	9
2.1 Руководящие документы	10
2.1.1 Указы президента Российской Федерации	10
2.1.2 Федеральные законы	10
2.1.3 Постановления правительства Российской Федерации.....	10
2.1.4 Прочие руководящие документы	11
3 План помещения	12
4 Анализ рынка средств защиты информации.....	16
4.1 Активная защита информации	16
4.2 Пассивная защита информации.....	19
5 Организация и стоимость защиты.....	21
Заключение.....	24
Список использованных источников.....	25

ВВЕДЕНИЕ

Современные предприятия сталкиваются с растущими вызовами в области обеспечения защиты информации. В свете постоянно усиливающихся угроз технической безопасности возникает неотложная необходимость в разработке и внедрении эффективных систем инженерно-технической защиты помещений. Целью настоящей курсовой работы является создание такой системы, направленной на предотвращение утечек информации, сведений ограниченного доступа, и обеспечение надежного сохранения государственной тайны с грифом "секретно".

Объектом исследования данной работы являются сами помещения предприятия, где хранится и обрабатывается конфиденциальная информация, а предметом – обеспечение безопасности этой информации в пределах данных помещений. В процессе исследования планируется провести анализ технических каналов, которые могут служить путями утечки информации, изучить существующие методы защиты от них, а также оценить соответствие действующей нормативно-правовой базы требованиям в области инженерно-технической защиты.

Кроме того, предстоит провести анализ организационной структуры предприятия и защищаемых помещений с целью выявления особенностей, влияющих на эффективность системы защиты. Выбор оптимальных технических средств также будет осуществлен путем анализа рынка средств технической защиты информации, учитывая специфику предприятия и его потребностей. В завершение работы планируется разработать смету на создание выбранной системы защиты, что даст предприятию возможность оценить финансовые затраты на внедрение предлагаемых мер безопасности.

Таким образом, данная курсовая работа нацелена на создание комплексного подхода к инженерно-технической защите помещений, в которых обрабатывается государственная тайна, и предоставление предприятию надежных инструментов для соблюдения высоких стандартов безопасности информации.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Наименование организации: StopY

Область деятельности: разработка и поддержка образовательной платформы в сфере ИБ для разработчиков, также тестирование систем на безопасность, в том числе государственных структур.

Основные информационные процессы и потоки в организации. Схема информационных процессов изображена на рис. 1.

Прибыль (месячная/годовая), расходы указаны ниже:

- прибыль: 75 млн руб в год
- расходы: 65 млн руб в год

статьи расходов:

- коммунальные платежи и аренда помещения — 4 млн в год;
- лицензионное ПО — 500 тыс. в год;
- обновление и ремонт техники — 1 млн в год;
- заработная плата сотрудников — 60 млн в год;
- изготовление брендированной продукции— 50 тыс. в год;
- командировки сотрудников — 100 тыс. в год.

Персонал организации (54 человека):

- СТО;
- CEO;
- Руководитель RnD;
- команда контента — 7 человек;
- команда разработки — 10 человек;
- отдел маркетинга — 5 человек;
- отдел дизайна — 8 человек;
- юридический отдел — 3 человека;
- финансовый отдел — 3 человека;
- отдел инфраструктуры — 5 человек;
- отдел ИБ — 5 человек;
- отдел поддержки — 5 человек.

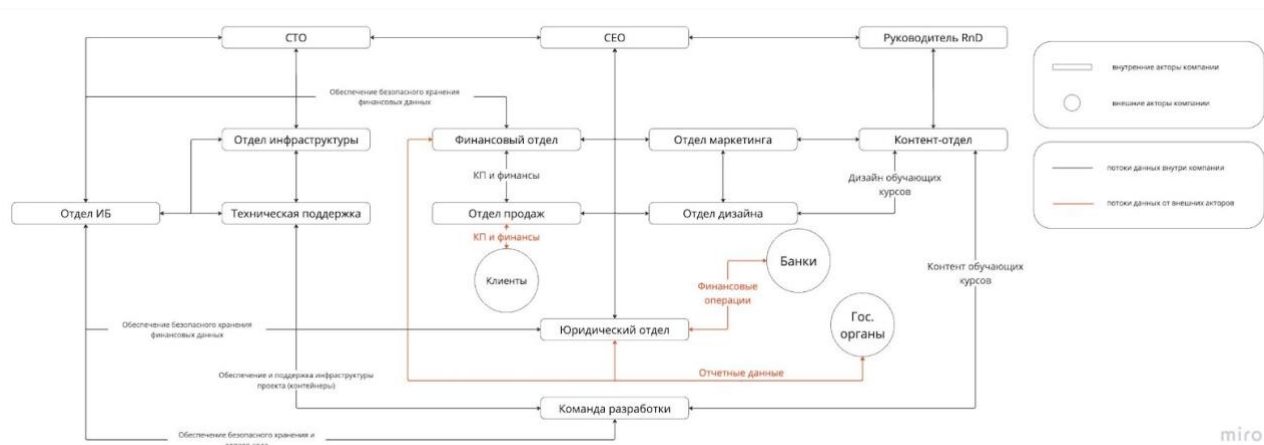


Рисунок 1 – Схема информационных потоков организации StopY

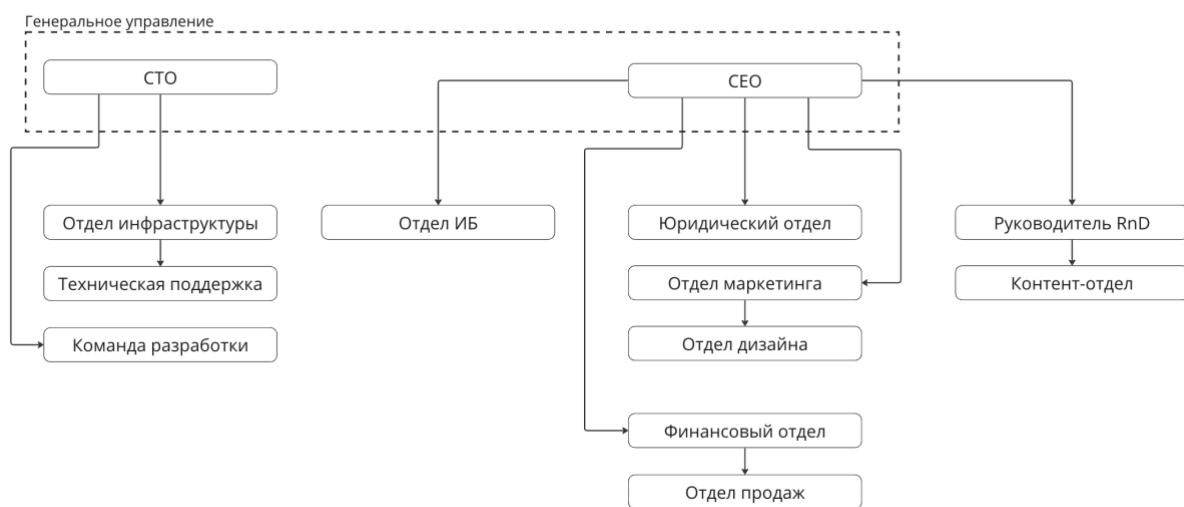


Рисунок 2 – Организационная схема предприятия

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно Руководящему документу Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В».

Согласно Постановлению правительства РФ №870 от 4 сентября 1995 г. (ред. 30 октября 2021 г.) уровень секретности определяется следующим образом:

1. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

2. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

3. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.

4. К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

5. К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

Ущерб безопасности Российской Федерации в данном контексте определяется как ущерб, причиненный интересам предприятия, учреждения или организации в различных

областях деятельности, таких как военная, внешнеполитическая, экономическая, научно-техническая, разведывательная, контрразведывательная и оперативно-розыскная.

Следовательно, уровень защищенности рассматриваемой организации определяется как 1В. Это объясняется тем, что предполагается обработка информации с грифом не выше "секретно", а предприятие функционирует как многопользовательская автоматизированная система, где не все пользователи обладают полными правами доступа ко всей информации.

2.1 Руководящие документы

2.1.1 Указы президента Российской Федерации

- Указ №1108 «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г.;
- Указ №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г.;
- Указ №1286 «Вопросы Межведомственной комиссии по защите государственной тайны» от 6 октября 2004 г.

2.1.2 Федеральные законы

- ФЗ №2446–1 «О безопасности» от 5 марта 1992 г.;
- ФЗ №5151–1 «О государственной тайне» от 21 июля 1993 г.;
- ФЗ №24 «Об информации, информатизации и защите информации» от 20 февраля 1995 г.

2.1.3 Постановления правительства Российской Федерации

- Постановление №333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г.;
- Постановление №870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г.;
- Постановление №608 «О сертификации средств защиты информации» от 26 июня 1995 г.;

- Постановление №63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" от 6 июня 2010 г.;

- Постановление №1205 "Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны" от 22 ноября 2012 г.

2.1.4 Прочие руководящие документы

- Приказ Минздравсоцразвития РФ № 989н "Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну" от 26 августа 2011 г.;

- СТР «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам»;

- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

- ГОСТ Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения».

3 ПЛАН ПОМЕЩЕНИЯ

План помещения представлен на рисунке ниже (рисунок 2). В таблице 1 представлено описание условных обозначений, представленных на плане.

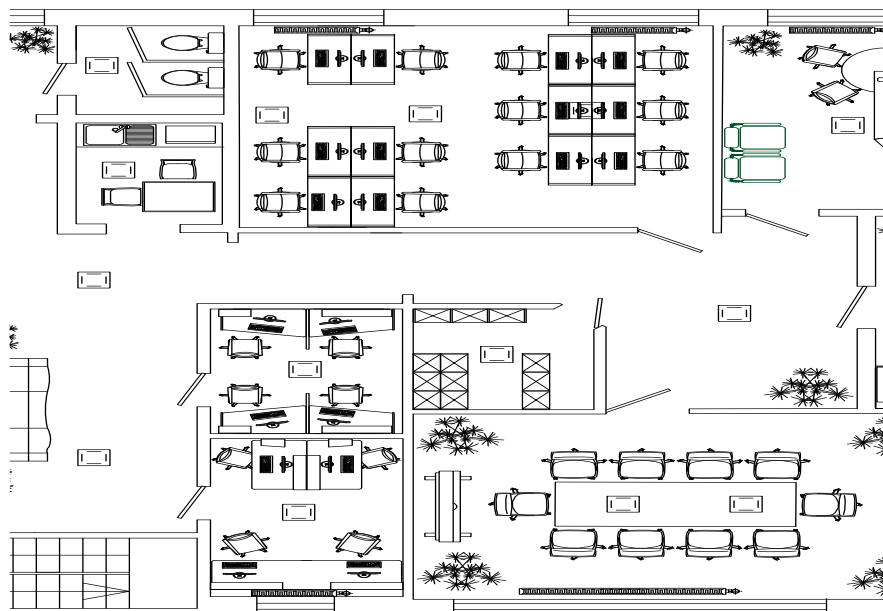
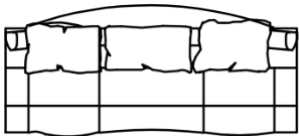









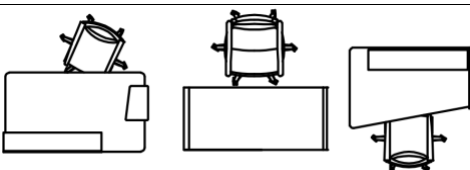
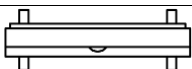
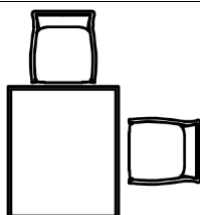
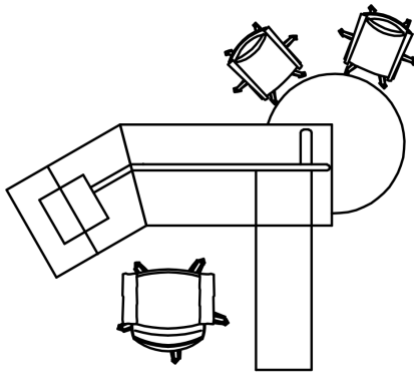


Рисунок 3 – План помещения

Таблица 1 – Условные обозначения с плана помещения

Обозначение	Описание
	Диван
	Раковины
	Унитаз
	СВЧ-Печь

Продолжение таблицы 1.

Обозначение	Описание
	Комнатные растения
	Шкафы для хранения документов
	Радиатор стальной
	Кресло
	Выход вентиляции
	Компьютер
	Офисные места
	Телевизор
	Кухонный стол
	Стол руководителя

Наиболее критичными для утечки государственной тайны являются следующие помещения: кабинет директора (справа снизу), переговорная (слева снизу), отдел разработки (справа посередине), архив (помещение посередине со шкафами), отдел информационной безопасности (над архивом), отдел инфраструктуры (слева сверху), юридический отдел (снизу по центру).

Офисное помещение расположено на шестом этаже бизнес-центра, являясь единственным офисом на данном этаже. Окна офиса не имеют смежности с эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, представляющими потенциальные точки вторжения посторонних лиц. Стены здания выполнены из железобетона и имеют толщину не менее 15 см, что обеспечивает дополнительный уровень безопасности.

Рассмотрим проблемы каждого из этих помещений:

- в кабинете директора располагаются 1 АРМ, 1 радиатор, 1 окно и 1 выход вентиляции;
- в переговорной располагаются 1 телевизор, 1 радиатор, 1 окно и 2 выхода вентиляции;
- в отделе разработки располагаются 12 АРМ, 2 радиатора, 2 окна и 3 выхода вентиляции;
- в архиве располагается 1 выход вентиляции;
- в отделе информационной безопасности располагаются 4 АРМ и 1 выход вентиляции;
- в отделе инфраструктуры располагаются 4 АРМ, 1 радиатор, 1 окно и 1 выход вентиляции;
- в юридическом отделе располагаются 5 АРМ, 2 радиатора, 2 окна и 2 выхода вентиляции.

Помимо этих помещений присутствуют:

- кухня для питания сотрудников с раковиной, СВЧ и 1 вентиляционным выходом;
- туалет с 2 раковинами, 2 унитазами, 1 окном, 1 радиатором и 1 вентиляционным выходом;
- коридор между помещениями, оборудованный диваном для посетителей и 3 вентиляционными выходами.

Таким образом, создадим перечень возможных технических каналов утечки информации:

- электрический;
- электромагнитный;
- акустический;
- акустоэлектрический;
- вибрационный;
- виброакустический;
- оптический.

Материально-вещественный канал утечки информации уже регулируется компанией и в рамках курсовой работы рассматриваться не будет.

4 АНАЛИЗ РЫНКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В таблице 2 описаны средства защиты информации, соотнесенные с каналом утечки информации, необходимые для обеспечения защиты от утечки информации ограниченного доступа – государственной тайны с грифом «секретно».

Таблица 2 – Каналы утечки и соответствующие средства защиты

Канал	Источник	Активная защита	Пассивная защита
Электромагнитный и электрический	Розетки, линии связи, АРМ, телевизор	Устройства электромагнитного зашумления	Фильтры сетей электропитания
Акустический и акустоэлектрический	Открытые окна и двери, тонкие стены, вентиляция проводка, «жучки»-микрофоны	Устройства акустического зашумления (акустоизлучатели), размыкатели слаботочных линий, средства обнаружения «жучков»	Использование звукоизоляционной обшивки, двойные двери с тамбуром, фильтры сетей электропитания, доводчики на дверях, замки на окнах
Вибрационный и виброакустический	Батареи, оконные стекла, вентиляция и другие твердые поверхности в помещении	Устройства вибрационного зашумления (виброизлучатели)	Использование звукоизоляционной обшивки, двойные двери с тамбуром, изоляция оконных стекол от рам с помощью резиновых прокладок, развязка труб при помощи мягких вставок
Оптический	Окна	Бликующие устройства	Жалюзи или плотные шторы, тонирующие пленки на окна

4.1 Активная защита информации

Далее в таблице 3 будут рассмотрены основные средства активной защиты информации от утечек по каналам, представленным в таблице 2.

Таблица 3 – Активные меры защиты информации

Наименование меры	Достоинства	Недостатки	Стоимость, руб.
Вибровозбудитель Соната СВ-4Б	Поддержка динамического изменение настроек СВАЗ	Максимальная продолжительность непрерывной работы – 8 часов	7 440
Виброизлучатель ВД-120	Продолжительность работы не ограничена	Нет динамического изменения настроек, система настраивается при установке	4 800
Вибровозбудитель ПЭД-8А	Входит в состав элементов системы «Шорох-5Л». Есть возможность настройки с помощью ПО «Шорох-ДУ».	Не было найдено	6 500
Вибровозбудитель СП-4Л (на ламели жалюзи)	Входит в состав элементов системы «Соната-АВ». Аналогов на рынке не найдено	—	840
Акустический излучатель «АИ-8А/Мини» (для установки в межрамное пространство)	Входит в состав элементов системы «Шорох-5Л». Аналогов на рынке не найдено	Не продается отдельно	—
Размыкатель линии Интернет Соната-ВК 4.3	Входит в состав элементов системы «Соната-АВ»	—	6 000
Размыкатель слаботочной линии Соната-ВК 4.3	Входит в состав элементов системы «Соната-АВ»	—	6 000
Управляемый размыкатель линии «Ключ-ВП(ИТ)»	Входит в состав элементов системы «Шорох-5Л»	Не продается отдельно	—

Продолжение таблицы 3

Наименование меры	Достоинства	Недостатки	Стоимость, руб.
Генератор шума ЛГШ-503	Широкий диапазон уровня шума. Возможность круглосуточного режима работы. Соответствие двум типам защиты – от наводок и от побочного ЭМИ	Удаленное управление возможно только в составе комплекса «Паутина»	44 200
Базовый генератор маскирующих радиопомех ГШ-111Б	Интерфейс для управления и контроля ГШ по сети Ethernet	Защита только от побочного ЭМИ	33 000
Средство активной защиты информации Соната-РЗ.1	Возможность повышения диапазона частот за счет дополнительной антенны	Максимальная продолжительность непрерывной работы – 8 часов	33 120
Нелинейный локатор PEGAS 2.0	Автоматическая регулировка мощности передатчика. Низкий вес прибора (0,95 кг)	Нет режима анализатора спектра	435 000
Нелинейный локатор ЛОРНЕТ-24	Низкий вес прибора (0.7 кг)	Отсутствие режима 20К	496 000
Нелинейный локатор NR-900EMS	Наличие разных режимов поляризации	Высокий вес прибора (3,7 кг)	471 000

Таким образом, были проанализированы активные меры защиты информации для предотвращения утечек по электрическим, электромагнитным, акустическим, акустоэлектрическим, виброакустическим, вибрационным каналам связи. Оптический канал будет защищен пассивными мерами. По результатам анализа было решено выбрать: комплекс Соната «АВ», включающий в себя вибровозбудители Соната СВ-4Б, вибровозбудители СП-4Л для установки на ламели жалюзи, размыкатели линии интернет Соната-ВК 4.3. Данные средства были выбраны в связи с хорошей работой в комплексе, также их можно закупать по отдельности. Помимо этого, было выбрано средство активной

защиты информации Соната-РЗ.1 (генератор шума), так как он при аналогичных характеристиках дешевле. Для поиска «жучков» было решено выбрать нелинейный локатор PEGAS 2.0 в связи с относительной дешевизной, удобством в использовании и легким весом.

4.2 Пассивная защита информации

Далее в таблице 4 будут рассмотрены основные средства активной защиты информации от утечек по каналам, представленным в таблице 2.

Таблица 4 – Пассивные меры защиты информации

Мера	Достоинства	Недостатки	Стоимость, руб
Тонирующие пленки на окна	Эффективно защищают от утечки по оптическому каналу, не требуют электропитания	Значительно ухудшают естественное освещение помещения, частая необходимость замен	От 500 руб. за кв.м
Жалюзи	Эффективно защищают как от утечки по оптическому каналу, так и по виброакустическому в комбинации с СП-4Л, не требуют электропитания	Ухудшают естественное освещение помещения, отсутствие защиты в открытом виде	От 1620 руб. за кв.м
Усиленные двери	Не требуют электропитания	—	от 30 000 руб.
Доводчики дверей	Низкая стоимость, увеличивают эффективность работы усиленных дверей	—	от 650 руб.
Замки для окон	Низкая стоимость, защита от открытия окон и утечки информации по акустическому каналу	Не защищают от утечки по виброакустическому каналу	от 400 руб.
Фильтры сети электропитания	Высокая эффективность	Высокая стоимость, сила тока только увеличивает цену	от 10 000 руб.

Таким образом, были проанализированы пассивные меры защиты информации для предотвращения утечки информации по оптическим, акустическим, виброакустическим и электромагнитным каналам связи. В результате анализа были выбраны жалюзи на окна, которые будут использоваться вместе с вибровозбудителями СП-4Л из предыдущего пункта. Так данные меры защиты информации будут в паре защищать два канала утечки информации, и при этом пропускать естественное освещение при необходимости. усиленные двери вместе с доводчиками для дополнительной защиты по акустическому каналу.

5 ОРГАНИЗАЦИЯ И СТОИМОСТЬ ЗАЩИТЫ

По результатам анализа рынка средств защиты информации были выбраны средства, стоимость для которых рассчитана в таблице 5.

Таблица 5 – Стоимость средств защиты информации

Средство	Количество	Стоимость, руб
Генераторный блок Соната АВ-4Л	1	10 320
Пульт управления Соната-ДУ 4.3	1	7 680
Блок электропитания и управления Соната ИП-4.3	1	21 600
Размыкатель линии Интернет Соната-ВК 4.3	27	162 000
Размыкатель слаботочной линии Соната-ВК 4.3	1	6 000
Вибровозбудитель Соната СВ-4Б	17	126 480
Вибровозбудитель Соната СП-4Л на ламели жалюзи	96	80 640
Средство активной защиты информации Соната-РЗ.1	6	198 720
Сетевой фильтр ЛФС-40-1Ф	3	210 600
Нелинейный локатор PEGAS 2.0	1	435 000
Жалюзи	24	48 000
Шумоизоляционная межкомнатная дверь ДГ-600 с доводчиком	7	280 000
Расходные монтажные материалы	-	5 000
Итого:		1 552 040

Таким образом, затраты на обеспечение инженерно-технической системы защиты информации получились 1 375 440 рублей. Учитывая доходы компании, затраты на организацию предложенной системы считаю оправданными. Размещение средств инженерно-технической защиты представлено на рисунке 3.

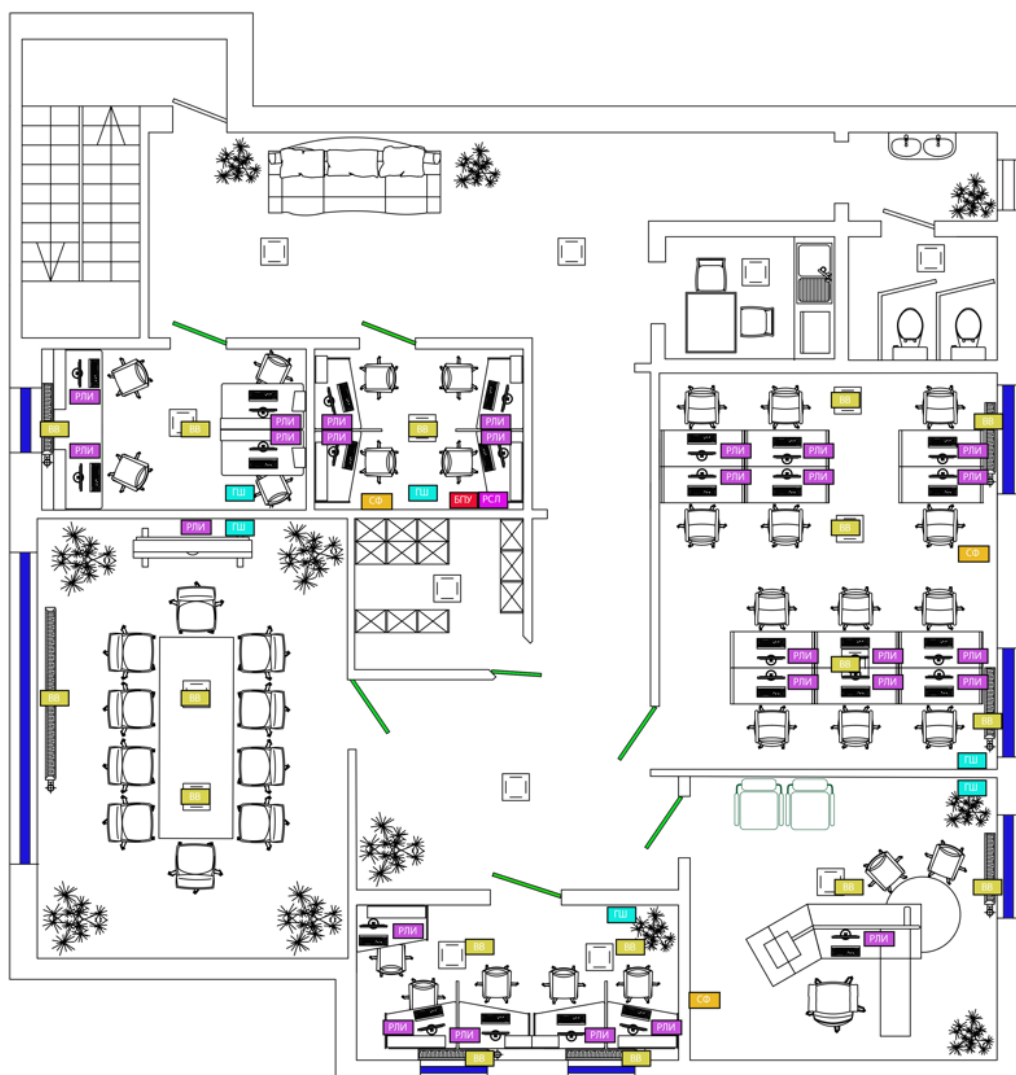






Рисунок 4 – Размещение средств защиты

Описание обозначений средств инженерно-технической защиты информации представлены в таблице 6.

Таблица 6 – Обозначения средств защиты

Обозначение	Описание
	Шумоизоляционная межкомнатная дверь ДГ-600 с доводчиком
	Жалюзи с вибровозбудителями Соната СП-4Л
	Средство активной защиты информации Соната-РЗ.1
	Размыкатель линии Интернет Соната-ВК 4.3

Продолжение Таблицы 6

Обозначение	Описание
	Вибровозбудитель Соната СВ-4Б
	Генераторный блок Соната АВ-4Л + Пульт управления Соната-ДУ 4.3 + Блок электропитания и управления Соната ИП-4.3
	Размыкатель слаботочной линии Соната-ВК 4.3
	Сетевой фильтр ЛФС-40-1Ф

ЗАКЛЮЧЕНИЕ

В процессе выполнения курсовой работы были осуществлены следующие шаги: проведено изучение каналов утечки информации и методов их предотвращения, проанализировано защищаемое помещение организации StopY с учетом его особенностей и расположения. Также был проведен анализ рынка технических средств пассивной и активной защиты.

На основе полученных данных была разработана система защиты конфиденциальной информации, включая государственную тайну, гриф "секретно". Дополнительно была проведена оценка стоимости внедрения предложенных мер безопасности, которая составила 1 552 040 рублей.

В результате моделирования защищаемых помещений были выявлены и успешно нейтрализованы различные технические каналы утечки информации, такие как электрический, электромагнитный, акустоэлектрический, оптический, акустический, вибрационный и виброакустический.

Таким образом, все задачи были выполнены, а цель курсовой работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. — 436 с.
2. Кармановский Н.С, Михайличенко О.В, Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие. — СПб: НИУ ИТМО, 2013. — 148 с.
3. Detector Systems / [Электронный ресурс] // [сайт]. — URL: <https://detsys.ru> (дата обращения: 30.11.2023).