

**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 118»***

**Выполнил:**

Магаськин К.А., 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**    Магаськин К.А.

(Фамилия И.О.)

**Факультет**    Безопасности информационных технологий

**Группа**    N34511

**Направление (специальность)**    Информационная безопасность

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

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

**Дисциплина**    Инженерно-технические средства защиты информации

**Наименование темы**    Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 118

**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**    Магаськин К.А.

(Фамилия И.О.)

**Факультет**    Безопасности информационных технологий

**Группа**    N34511

**Направление (специальность)**    Информационная безопасность

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

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

**Дисциплина**    Инженерно-технические средства защиты информации

**Наименование темы**    Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 118

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу	21.10.2023	21.10.2023	
2	Анализ материалов	13.11.2023	13.11.2023	
3	Написание курсовой работы	26.11.2023	26.11.2023	
4	Подготовка презентации	3.12.2023	3.12.2023	
5	Защита курсовой работы	11.12.2023	11.12.2023	

**Руководитель** \_\_\_\_\_

(Подпись, дата)

**Студент**    

(Подпись, дата)

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

Студент Магаськин К.А.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 118

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

**2. Характер работы**

☐ Расчет

☒ Конструирование

☐ Моделирование

☐ Другое:

**3. Содержание работы**

Курсовая работы включает разделы: введение, теоретическая часть, анализ защищаемых помещения, выбор средств защиты информации, 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)

«21» октября 2023 г.

## СОДЕРЖАНИЕ

Введение .....	6
1 Теоретическая информация .....	7
1.1 Технические каналы утечки информации .....	7
1.1.1 Каналы утечки акустической информации .....	7
1.1.2 Каналы утечки информации по линиям связи .....	9
1.2 Методы защиты от утечек информации по техническим каналам .....	9
1.2.1 Организационно-режимные мероприятия .....	9
1.2.2 Поисковые мероприятия .....	10
1.2.3 Технические мероприятия .....	10
1.3 Руководящие документы .....	11
1.3.1 Федеральные законы .....	11
1.3.2 Указы Президента Российской Федерации .....	12
1.3.3 Постановления Правительства Российской Федерации .....	12
1.3.4 Приказы и другие документы отраслевых регуляторов, стандарты .....	12
2 Анализ предприятия и защищаемых помещений .....	14
2.1 Обоснование защиты информации .....	14
2.2 Организационная структура предприятия .....	15
2.3 Анализ помещений .....	16
3 Анализ рынка средств защиты информации .....	19
3.1 Пассивные меры защиты информации .....	20
3.2 Активные меры защиты информации .....	21
4 Внедренные меры защиты .....	24
Заключение .....	27
Список использованных источников .....	28

## ВВЕДЕНИЕ

В современном мире успешная деятельность предприятий, работающих с государством, зачастую тесно связана с обеспечением безопасности информации, составляющей государственную тайну. Раскрытие информации ограниченного доступа может не только подорвать финансовую стабильность компании, но и повредить ее репутации и даже нанести ущерб интересам государства. Именно поэтому вопрос инженерно-технической защиты информации в помещениях является актуальной темой исследования.

Для предотвращения утечек информации ограниченного доступа требуется комплексный подход, включающий в себя организационно-правовые, программно-аппаратные, инженерно-технические и криптографические меры. Особое внимание должно уделяться инженерно-техническим мерам, предотвращающим съём информации по техническим каналам утечки информации. Эти каналы утечки информации в дальнейшем будут рассмотрены в курсовой работе.

Цель данной курсовой работы – разработка системы инженерно-технической защиты помещений предприятия от утечек информации, составляющей государственную тайну с грифом «секретно». Объектом исследования являются сами помещения, а предметом – обеспечение безопасности информации ограниченного доступа в его пределах.

В рамках работы планируется изучение технических каналов утечки информации, методов защиты от них, а также изучение нормативно-правовой базы, регламентирующей инженерно-техническую защиту помещений, анализ организационной структуры предприятия и защищаемых помещений, выбор оптимальных технических средств путем анализа рынка средств технической защиты информации и разработка сметы на создание выбранной системы защиты.

# **1 ТЕОРЕТИЧЕСКАЯ ИНФОРМАЦИЯ**

## **1.1 Технические каналы утечки информации**

Технический канал утечки информации (ТКУИ) представляет собой сложную систему, объединяющую источник конфиденциальной информации, среду распространения и средства технической разведки (ТСР), предназначенные для перехвата данных. Существует множество технических каналов, классифицируемых по физическим свойствам и принципам функционирования.

Виды каналов:

- акустические (запись звука, подслушивание и прослушивание);
- акустоэлектрические (звуковые волны с дальнейшей передачей ее через сети электропитания);
- виброакустические (воздействие акустического сигнала на строительные конструкции и инженерно-технические коммуникации защищаемых помещений);
- оптические (фотографирование, видеосъемка, наблюдение);
- электромагнитные (копирование полей путем снятия индуктивных наводок);
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладных устройств», далее - ЗУ), модулированные информативным сигналом;
- материальные (бумажные и иные носители информации).

Технические каналы утечки информации подразделяются на естественные и искусственные. Естественные каналы возникают при обработке информации техническими средствами, например, электромагнитные каналы утечки информации. Искусственные каналы создаются злоумышленниками преднамеренно, например с помощью электронных устройств перехвата информации (закладных устройств).

Рассмотрим описанные выше каналы утечки информации с двух сторон: утечки акустической (речевой информации), например во время переговоров и утечки информации по каналам связи.

### **1.1.1 Каналы утечки акустической информации**

К техническим каналам утечки акустической информации в зависимости от среды передачи относятся следующие:

- акустический (воздушный);

- виброакустический (структурный);
- акустоэлектрический;
  - «микрофонный эффект»;
- микрофон и передатчик (ЗУ);
- стетоскоп и передатчик (ЗУ);
- высокочастотное облучение (полуактивное ЗУ, основанное на высокочастотном навязывании).

В акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. Для перехвата информации могут использоваться миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы, окна), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны-стетоскопы.

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через вспомогательные технические устройства, обладающие «микрофонным эффектом, либо с помощью ВЧ-навязывания.

«Микрофонный эффект» — это нежелательное явление, при котором некоторая часть электрической цепи воспринимает звуковые колебания и вибрацию подобно микрофону. Чаще всего возникает при изменении ёмкости, особенно в высокочастотных цепях, где даже незначительные колебания плохо закреплённых деталей могут существенно повлиять на параметры прохождения основного сигнала.

ВЧ-воздействие (навязывание) - способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства. Он заключается в модуляции электромагнитного зондирующего сигнала речевым в результате их одновременного воздействия на элементы обстановки или специально внедренные устройства. Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.



### **1.1.2 Каналы утечки информации по линиям связи**

К техническим каналам, связанным с передачей информации по линиям связи относят:

- электрический;
- электромагнитный;

ПЭМИН (побочные электромагнитные излучения и наводки) – это случайные опасные сигналы, возникающие во время работы в выделенном помещении радиосредств и электрических приборов. Причины возникновения ПЭМИН:

- не предусмотренные функциями радиосредств и электрических приборов преобразования внешних акустических сигналов в электрические сигналы;
- паразитные связи и наводки;
- побочные НЧ- и ВЧ-излучения.

Паразитная генерация усилителей возникает из-за неконтролируемой положительной обратной связи с конструктивными особенностями схемы или старением элементов. Для защиты от утечки информации за счет паразитной генерации применяется контроль усилителей на самовозбуждение с помощью радиоприемников типа «индикаторов поля», работающих в достаточно широком диапазоне частот, за счет чего обеспечивается поиск опасного сигнала.

## **1.2 Методы защиты от утечек информации по техническим каналам**

В зависимости от целей, порядка проведения и применяемого оборудования методы и способы защиты информации от утечки по ТКУИ в целом можно разделить на три вида: организационно-режимные, поисковые и технические.

### **1.2.1 Организационно-режимные мероприятия**

Организационно-режимные мероприятия осуществляются в основном без применения технических средств и включают в себя:

- определение границ контролируемой зоны (КЗ) вокруг объекта и обеспечение режимного ограничения доступа на объекты размещения технических средств приема, обработки, хранения и передачи информации, а также в выделенные помещения;
- введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации;

- отключение на период проведения закрытых совещаний вспомогательных технических средств и систем, обладающих качествами электроакустических преобразователей, от соединительных линий;
- привлечение к строительству и реконструкции защищаемых помещений, монтажу аппаратуры ТСПИ, а также к работам по защите информации организаций, лицензированных соответствующими службами на деятельность в данной области;
- использование только сертифицированных устройств;
- категорирование и аттестация объектов информатизации на соответствие требованиям обеспечения защиты информации при проведении работ со сведениями различной степени секретности.

### **1.2.2 Поисковые мероприятия**

Поисковые мероприятия осуществляются с применением специальных поисковых приборов, зачастую с привлечением специалистов сторонних организаций и включают в себя:

- выявление каналов утечки – активные проверки с использованием пассивных и активных поисковых средств, включая проверку обрабатываемых ТСПИ, выявление каналов утечки речевой, видовой информации и информации, передаваемом по линиям связи;
- выявление закладных устройств с помощью контроля радиоспектра и побочных электромагнитных излучений ТСПИ, в том числе с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров или программно-аппаратных комплексов;
- проверку выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок.

### **1.2.3 Технические мероприятия**

Технические мероприятия по защите информации проводятся с применением как пассивных, так и активных защитных приемов и средств.

К пассивным техническим способам защиты относят:

- установку комплексных систем защиты от несанкционированного физического доступа (НСД) на ТСПИ и кабельные линии связи;
- экранирование ВП, ТСПИ и отходящих от них соединительных линий;
- заземление ТСПИ и экранов соединительных линий приборов;

- звуко- и виброизоляция механических узлов ТСПИ;
- встраивание специальных фильтров в ВТСС, обладающих “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны;
- использование специальных конструкций оконных блоков, специальных пленок, жалюзей и штор;
- установку автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ;
- монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров;
- звуко- и виброизоляцию защищаемых помещений;
- разводку труб мягкими вставками с целью виброизоляции.

К активным техническим мерам защиты каналов утечки информации относят:

- пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ;
- акустическое и вибрационное зашумление строительных конструкций;
- СВЧ-воздействие на микрофонные цепи (подавление диктофонов устройствами направленного высокочастотного радиоизлучения);
- зашумление каналов передачи данных;
- зашумления силовой сети и цепей заземления;
- разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств)
- установка систем гарантированного уничтожения информации;
- шифрование информации, передаваемой по каналам связи.

### **1.3 Руководящие документы**

Рассмотрим документы, регламентирующие инженерно-техническую защиту помещений, в которых обрабатывается информация, составляющая государственную тайну.

#### **1.3.1 Федеральные законы**

- ФЗ №2446–1 «О безопасности» от 5 марта 1992 г.;
- ФЗ № 4524–1 «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г.;
- ФЗ №5151–1 «О государственной тайне» от 21 июля 1993 г.;
- ФЗ №15«О связи» от 16 февраля 1995 г.;

- ФЗ №24 «Об информации, информатизации и защите информации» от 20 февраля 1995 г.;
- ФЗ №85 «Об участии в международном информационном обмене» от 4 июля 1996 г.

### **1.3.2 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 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» от 16 августа 2004 г.;
- Указ №1286 «Вопросы Межведомственной комиссии по защите государственной тайны» от 6 октября 2004 г.

### **1.3.3 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.;

### **1.3.4 Приказы и другие документы отраслевых регуляторов, стандарты**

- СТР «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам»;
- руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

- 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».

## **2 АНАЛИЗ ПРЕДПРИЯТИЯ И ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ**

### **2.1 Обоснование защиты информации**

Объектом защиты является компания ООО «Пенькоф» (далее – Компания), занимающаяся разработкой программного обеспечения преимущественно по заказу как от корпоративных клиентов, так и от государственных структур. Основным видом деятельности организации является издание прочих программных продуктов (ОКВЭД 58.29).

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». Важно отметить, что ГОСТ Р 57429–2017 определяет средство вычислительной техники как «совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем».

В соответствии с Постановлением Правительства РФ от 4 сентября 1995 г. N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" к секретным сведениям следует относить все сведения, отличные от сведений:

1. особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.
2. совершенно секретных: сведений 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.

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-розыскной области деятельности.

Таким образом класс защищенности у рассматриваемой организации 1В, так как предполагается, что в ней обрабатывается информация с грифом не выше «секретно» и предприятие является многопользовательской АС, где не все пользователи имеют права доступа ко всей информации. В случае реализации угрозы ущерб будет нанесен лишь интересам предприятия научно-технической деятельности.

## 2.2 Организационная структура предприятия

В Компании работает 70 человек, организационная структура предприятия показана на рисунке 1.

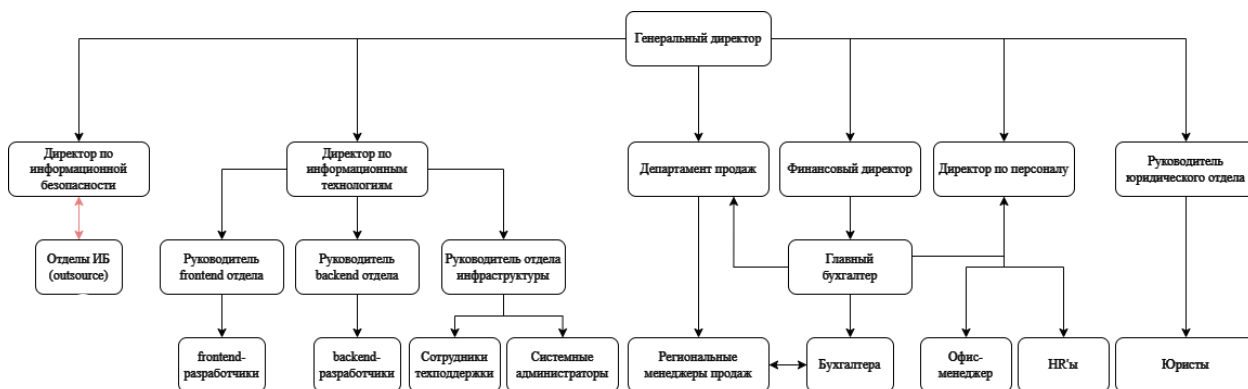


Рисунок 1 – Организационная структура Компании

На рисунке 2 представлена схема информационных потоков Компании. Зеленым цветом обозначены внешние открытые потоки, красным – закрытые, черным – внутренние, не содержащие информации ограниченного доступа.

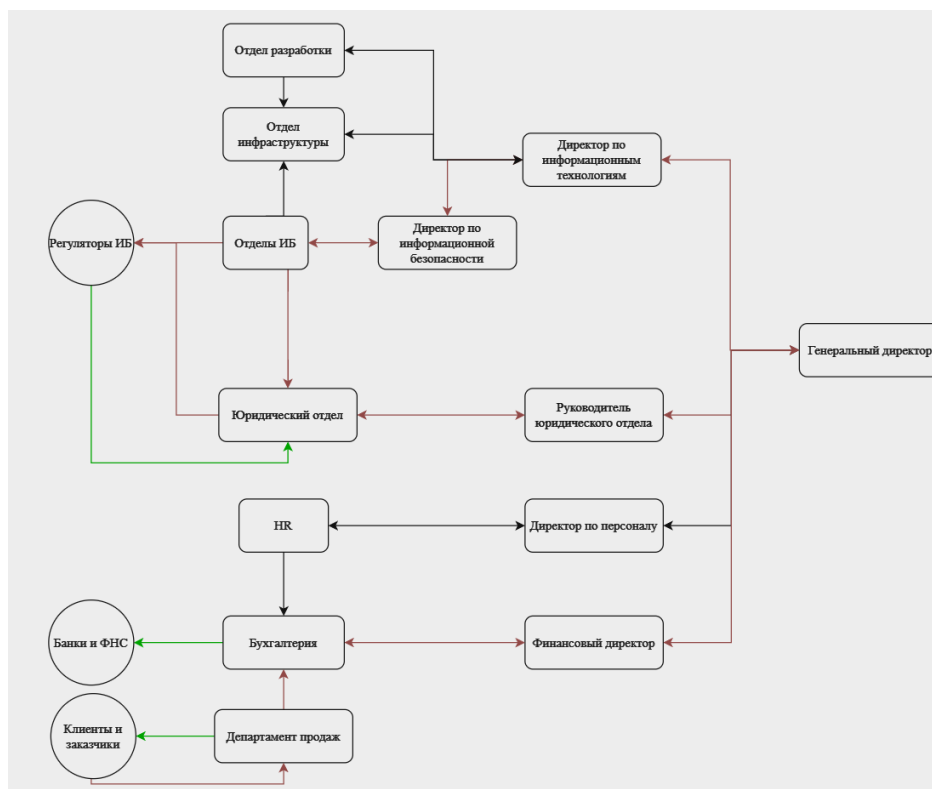


Рисунок 2 – Информационные потоки Компании

Прибыль (месячная) и расходы:

- прибыль (общая) – 10650 тыс/мес;
- прибыль (чистая) - 4500 тыс/мес;
- расходы – 6150 тыс/мес:
  - общий фонд оплаты труда - 4500 тыс/мес;
  - коммунальные платежи и аренда помещения - 600 тыс/мес;
  - услуги сторонней организации по ИБ - 600 тыс/мес;
  - аренда серверов – 210 тыс/мес;
  - лицензии на ПО - 120 тыс/мес;
  - прочие расходы - 120 тыс/мес.

### 2.3 Анализ помещений

На рисунке 3 представлен план помещений офиса Компании.



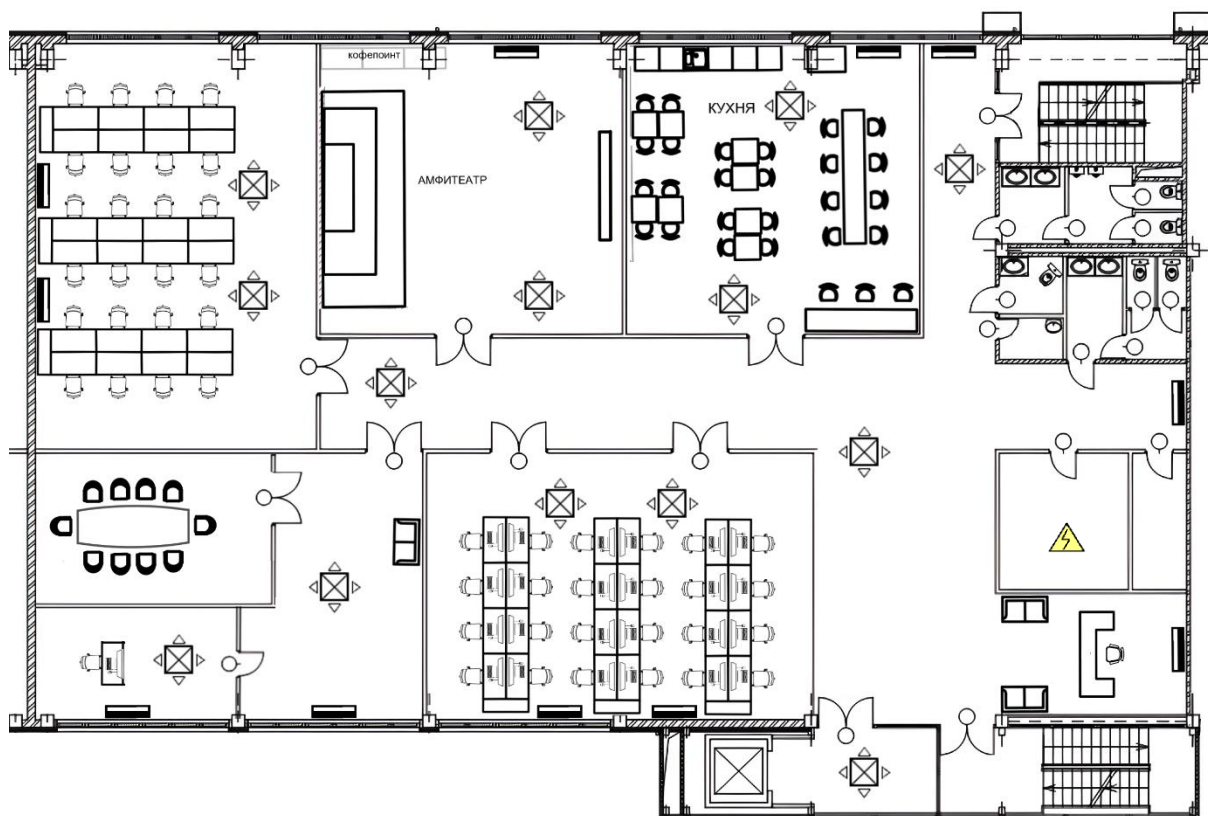


Рисунок 3 – План помещений

Наиболее критичными для утечки государственной тайны являются следующие помещения: кабинет директора, переговорная комната (слева снизу), отдел бухгалтерии и амфитеатр (слева сверху), а также отдел разработчиков (снизу по центру). Офис располагается на 4 этаже бизнес-центра, других офисов на этаже нет. Окна офиса не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания железобетонные, толщиной не менее 15 см. Большинство внутренних перегородок сделаны из гипсокартона без звукоизоляционного слоя.

Рассмотрим наиболее важные факторы каждого из помещений:

- в кабинете директора располагается 1 окно, 1 батарея, 1 АРМ, телефон и 1 выход вентиляции;
- переговорная имеет достаточно тонкие стены и граничит с помещением бухгалтерии;
- в отделе бухгалтерии имеются 2 батареи, 2 окна и 2 выхода вентиляции, а также некоторое число телефонов;
- в отделе разработчиков имеются 2 батареи, 1 окно и 2 выхода вентиляции, а также 24 АРМ, помещение имеет тонкие стены, граничащие с коридором;

– в амфитеатре тонкие стены граничат с кухней и отделом бухгалтерии, имеется 1 окно, 2 выхода вентиляции, батарея, а также медиаэкран с выходом в Интернет.

Таким образом, создадим перечень возможных технических каналов утечки информации:

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

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

### 3 АНАЛИЗ РЫНКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Для обеспечения защиты от утечки информации ограниченного доступа – государственной тайны с грифом «секретно» по выявленным техническим каналам утечки, требуется оснастить помещения средствам защиты, приведенными в таблице 1.

Таблица 1 – Каналы утечки и соответствующие им средства защиты

Канал	Источник	Пассивная защита	Активная защита
Акустический и акустоэлектрический	Открытые окна и двери, тонкие стены, вентиляция проводка, «жучки»-микрофоны	Использование многослойных акустически неоднородных конструкций с упругими прокладками, двойные двери с тамбуром, фильтры сетей электропитания, доводчики на дверях, замки на окнах	Устройства акустического зашумления (акустоизлучатели), издающие «белый» и «розовый» шумы, размыкатели слаботочных линий, средства обнаружения «жучков»
Вибрационный и виброакустический	Батареи, оконные стекла, вентиляция и другие твердые поверхности в помещении	Использование многослойных акустически неоднородных конструкций с упругими прокладками, двойные двери с тамбуром, изоляция оконных стекол от рам с помощью резиновых прокладок, тройное остекление, развязка труб при помощи мягких вставок	Устройства вибрационного зашумления (виброизлучатели)
Электромагнитный и электрический	Розетки, линии связи (в том	Фильтры сетей электропитания	Устройства электромагнитного зашумления

	числе Ethernet), АРМ		
Оптический	Окна	Жалюзи/шторы, тонирующие пленки на окна	Бликующие устройства

### 3.1 Пассивные меры защиты информации

Анализ рынка пассивных мер защиты информации представлен в таблице 2.

Таблица 2 – Пассивные меры защиты информации

Наименование меры	Достоинства	Недостатки	Стоимость
Шумоизоляция поверхностей помещения (стены, пол, потолок)	Не требует электропитания и обслуживания.	Высокая стоимость, иногда отсутствие возможности возводить конструкции в арендуемом помещении	Зависит от площади поверхностей помещения, от 6000 руб за кв.м
Тонирующие пленки на окна	Не требуют электропитания, эффективно защищает от утечки по оптическому каналу	Значительно ухудшает освещенность помещения солнечным светом, со временем изнашивается, подвержена механическим повреждениям	Зависит от площади окон, от 1100 руб. за кв.м
Жалюзи/шторы	Защищают как от утечки по оптическому каналу, так и частично по виброакустическому каналу, не требуют электропитания	Ухудшают освещенность помещения солнечным светом, почти не защищают от утечки, когда находятся в открытом виде	Зависит от площади окон, от 1600 руб. за кв.м

Усиленные двери	Не требуют электропитания и обслуживания.	Высокая стоимость, иногда отсутствие возможности вносить значительные изменения в арендуемое помещение	от 40 000 руб.
Доводчики дверей	Увеличивают эффективность работы усиленных дверей	-	от 791 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.
Развязка труб мягкими вставками	Низкая стоимость	Эффективность ниже, чем у активного шумления, иногда отсутствие возможности вносить изменения в коммуникации арендуемого помещения	от 1000 руб.
Фильтры сети электропитания	Высокая эффективность	Высокая цена, растущая с силой тока в сети, максимум 200 А	от 40 000 руб.

Таким образом, из пассивных мер защиты информации было решено выбрать: шумоизоляцию поверхностей защищаемого помещения, оставить уже имеющиеся в офисе жалюзи на окна, а также установить усиленные двери с доводчиками в защищаемые помещения.

### 3.2 Активные меры защиты информации

Анализ рынка активных мер защиты информации приведен в таблице 3.

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
Размыкатель телефонной линии Соната-ВК 4.1	Входит в состав элементов системы «Соната-АВ».	Нет	6 000
Размыкатель слаботочной линии Соната-ВК 4.2	Входит в состав элементов системы «Соната-АВ».	Нет	6 000
Размыкатель линии Интернет Соната- ВК 4.3	Входит в состав элементов системы «Соната-АВ».	Нет	6 000
Вибровозбудитель СП-4Л (на ламели жалюзи)	Входит в состав элементов системы «Соната-АВ». Аналогов на рынке не найдено.	Нет	840
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	Интерфейс для управления и контроля ГШ по сети Ethernet	Защита только от побочного ЭМИ	33 000

радиопомех ГШ-111Б			
Нелинейный локатор PEGAS 2.0	Автоматическая регулировка мощности передатчика. Низкий вес прибора (0,95 кг)	Нет режима анализатора спектра	435 000
Нелинейный локатор NR-900EMS	Более высокая чувствительность приемника	Высокий вес прибора (3,7 кг)	471 000

Таким образом, из активных мер защиты информации было решено выбрать: комплекс Соната «АВ», включающий в себя вибровозбудители Соната СВ-4Б, вибровозбудители СП-4Л, размыкатели телефонной линии Соната-ВК 4.1, а также размыкатели слаботочной линии Соната-ВК 4.2 и размыкатели линии интернет Соната-ВК 4.3. Также в дополнение к комплексу было решено поставить генераторы шума ЛГШ-503 в каждое защищаемое помещение. Для поисковых мероприятий был выбран нелинейный локатор PEGAS 2.0.

#### 4 ВНЕДРЕННЫЕ МЕРЫ ЗАЩИТЫ

По результатам анализа рынка средств защиты информации были выбраны средства, приведенные в таблице 4.

Таблица 4 – Средства защиты информации и их итоговая стоимость.

Средство	Количество	Стоимость, руб
Размыкатель телефонной линии Соната-ВК 4.1	13	78 000
Размыкатель слаботочной линии Соната-ВК 4.2	5	30 000
Размыкатель линии Интернет Соната-ВК 4.3	26	156 000
Вибровозбудитель Соната СП-4Л на ламели жалюзи	180	151 200
Генераторный блок СонатаАВ-4Л	5	51 600
Пульт управления Соната-ДУ 4.3	5	38 400
Блок электропитания и управления Соната ИП-4.3	5	108 000
Вибровозбудитель Соната СВ-4Б	13	96 720
Генератор шума ЛГШ-503	5	221 000
Нелинейный локатор PEGAS 2.0	1	435 000
Гипсоволокнистый лист ГВЛВ ПК 12.5 мм Knauf Суперлист 1200x2500 мм	85	103 700
Герметик звукоизоляционный Вибросил 290мл	60	43 800
Звукоизоляционная лента Вибростек-М100	20	49 360
Панель звукоизоляционная ЗИПС-III Ультра 1.2x0.6 м	350	1 051 920
Дверь звукоизолированная усиленная ПГ 1001 SP	9	414 855
Расходные монтажные материалы	-	10 000
Работы по монтажу звукоизоляции	-	250 760
Итого:		3 290 315

Таким образом, итоговая стоимость системы защиты от утечки по техническим каналам утечки информации составила 3 290 315 руб. С учетом доходов Компании, полагаем затраты на представленную систему подъемными и оправданными обрабатываемым классом информации ограниченного доступа.

Размещение средств защиты информации показано на рисунке 4.



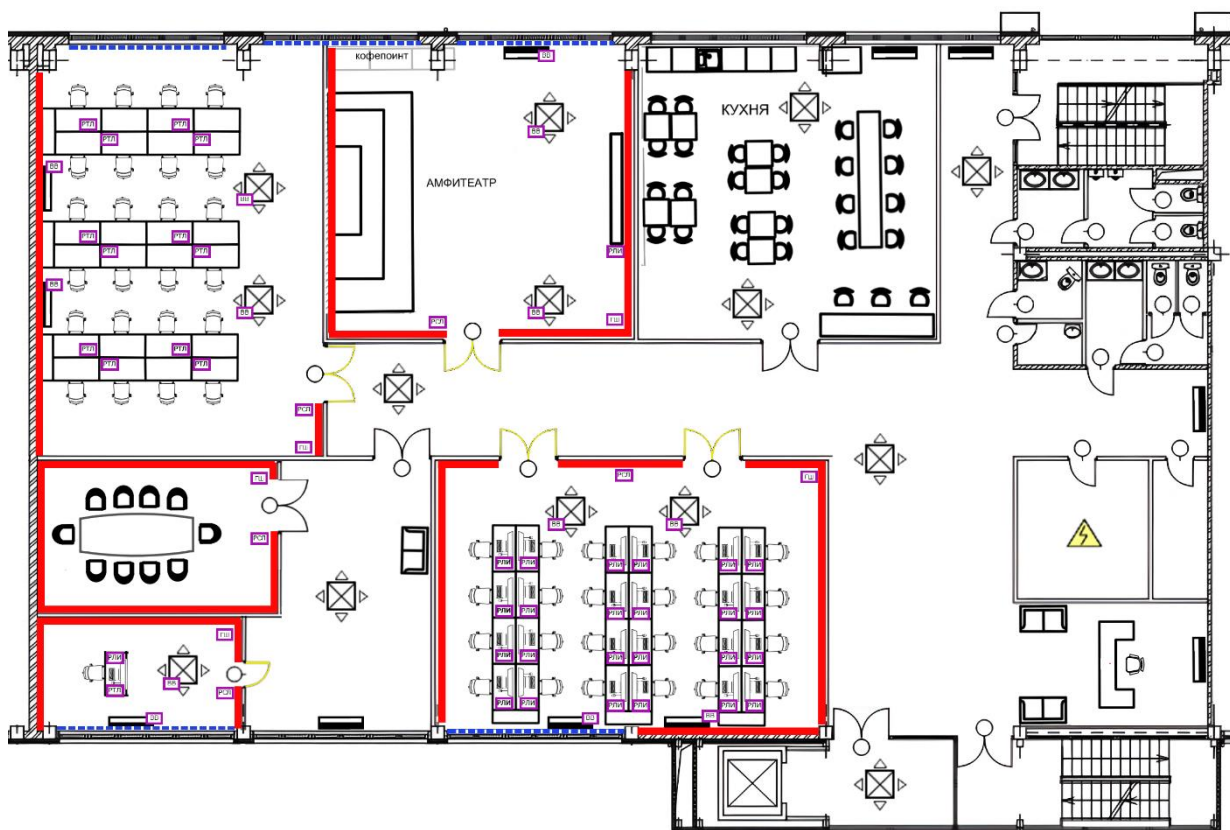






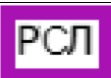


Рисунок 4 – Размещение средств защиты информации.

Легенда плана представлена в таблице 5.

Таблица 5 – Легенда плана размещения средств защиты информации.

Обозначение	Описание
	Стена со звукоизоляционной обшивкой
	Усиленная дверь
	Окно-жалюзи с вибровозбудителем «СП-4Л»
	Генератор шума
	Размыкатель линии Интернет
	Вибровозбудитель

	Размыкатель телефонной линии
	Размыкатель слаботочной линии

## **ЗАКЛЮЧЕНИЕ**

В рамках курсовой работы были изучены каналы утечки информации и способы ее предотвращения, проведен анализ защищаемого помещения организации ООО «Пенькоф» с учетом его особенностей и расположения, изучен рынок технических средств пассивной и активной защиты, разработана система защиты конфиденциальной информации (коммерческой тайны), а также проведена оценка стоимости введения предложенных мер. Итоговая стоимость предложенных мер составила 3 290 315 руб.

В результате моделирования защищаемых помещений были выявлены и нейтрализованы следующие ТКУИ:

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

Таким образом, все задачи, поставленные в рамках курсового проекта, были выполнены в полном объеме, а цель достигнута.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ворона В. А., Костенко В. О. Способы и средства защиты информации от утечки по техническим каналам [Текст] / Ворона В. А., Костенко В. О. // Computational nanotechnology. — 2016. — № 3;
2. Ларионцева Е. А. Основные виды каналов утечки информации [Текст] / Ларионцева Е. А. // Машиностроение и компьютерные технологии. — 2011. — № 3;
3. ООО "Детектор Системс" Антипрослушка - защита переговоров и помещений от прослушивания / ООО "Детектор Системс" [Электронный ресурс] // Detector Systems : [сайт]. — URL: <https://detsys.ru/article/zaschita-ot-proslushivaniya> (дата обращения: 24.11.2023);
4. Дуплянкин А. 04.35 Защищаемое помещение, информативный сигнал (определения). Защита от утечки речевой информации (подробно: организационные и технические (пассивные и активные) методы по всем (8-ми каналам) утечки / Дуплянкин А. [Электронный ресурс] // Сайт Андрея : [сайт]. — URL: [https://www.gman1990.ru/articles.php?article\\_id=56](https://www.gman1990.ru/articles.php?article_id=56) (дата обращения: 27.11.2023).