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 системы защиты от утечки информации по различным каналам»

Выполнил(а):
Тетерина Александра Викторовна, студентка группы N34511

(подпись)

Проверил преподаватель:
Попов Илья Юьевич, к.т.н., доцент ФБИТ

(подпись)

Отметка о выполнении:

Санкт-Петербург
2023

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Тетерина Александра Викторовна

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 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

Задание Проанализировать схему помещений предприятия и технические каналы утечки информации и разработать инженерно-техническую систему защиты информации для предприятия

Краткие методические указания

Содержание пояснительной записки

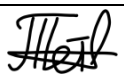
Курсовая работа состоит из следующих разделов:

Введение, анализ и классификация технических каналов утечки информации, анализ исследуемого предприятия, свод регулирующих документов в области применения мер защиты информации, анализ помещений предприятия, анализ рынка продуктов защиты информации, разработка инженерно-технической системы защиты информации для предприятия.

Рекомендуемая литература

Руководитель _____

(Подпись)

Студент 

(Подпись)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Тетерина Александра Викторовна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 Информационная безопасность

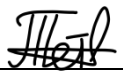
Руководитель Попов И.Ю., к.т.н., доцент ФБИТ
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	25.10.2023	25.10.2023	
2	Создание плана курсовой работы	15.11.2023	15.11.2023	
3	Анализ теоретической составляющей	23.112023	23.11.2023	
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	9.12.2023	9.12.2023	
5	Презентация КР перед аудиторией	19.12.2023	19.12.2023	

Руководитель _____
(Подпись)

Студент 
(Подпись)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Тетерина Александра Викторовна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 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 безопасности в финансовой организации

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом ☐ Сформулированы при участии студента ☒ Определены руководителем

Цель работы – разработка инженерно-технической системы защиты информации для предприятия.

2. Характер работы

☐ Расчет ☐ Конструирование ☐ Моделирование ☒ Другое

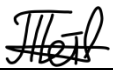
3. Содержание работы

В данной курсовой представлен анализ технических каналов утечки информации, анализ рынка средств защиты информации и разработка инженерно-технической системы защиты информации для конкретного предприятия с предварительным его анализом.

4. Выводы

В результате выполнения работы был проведён анализ предприятия и разработана инженерно-техническая система защиты информации для него.

Руководитель _____
(Подпись)

Студент 
(Подпись)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном информационном обществе, где обмен конфиденциальной информацией является повсеместным, вопросы обеспечения ее безопасности приобретают стратегическое значение. С ростом сложности информационных технологий и расширением способов взаимодействия с данными, необходимость в разработке эффективных систем защиты становится критической для бизнеса, государственных структур, а также для обычных пользователей.

Данная курсовая работа посвящена проблеме проектирования системы защиты от утечки информации по различным каналам в контексте инженерно-технических средств защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из девяти помещений и представляет собой офис предприятия с кабинетом директора, кабинет секретаря, кабинетом бухгалтера, переговорной, двумя рабочими кабинетами, архивом, уборной и прихожей.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Канал утечки информации – это совокупность источника информации, материального носителя (или среды распространения несущего эту информацию сигнала) и средства выделения информации из сигнала или носителя.

Классификация каналов утечки информации представлены на Рисунке 1.

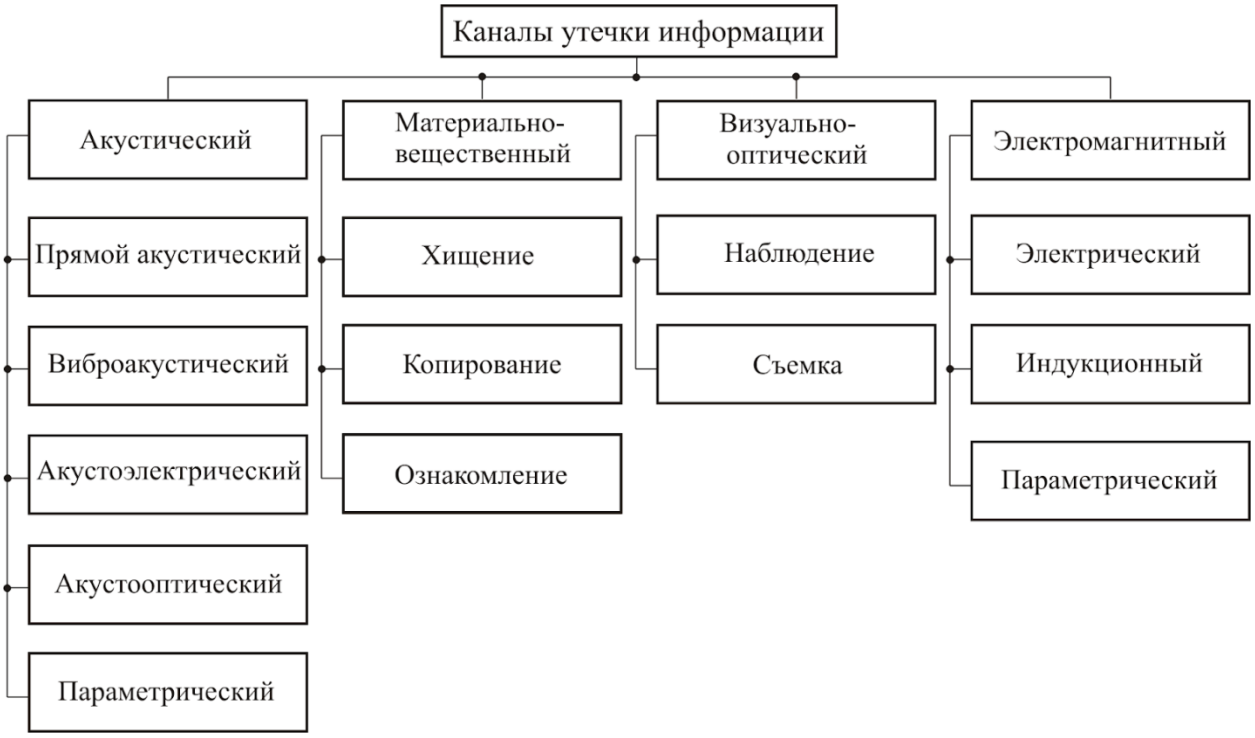


Рисунок 1 - Классификация каналов утечки информации

1.1. Акустический канал

Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по телефону;
- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;
- приемника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Акустические каналы утечки информации могут быть следующих видов:

1) прямой акустический – в прямых акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. В качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический. Перехват акустической (речевой) информации из выделенных помещений по данному каналу может осуществляться: с использованием портативных устройств звукозаписи (диктофонов), скрытно установленных в выделенном помещении, с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной среде), скрытно установленных в выделенном помещении, с передачей информации по радиоканалу, оптическому каналу, электросети 220 В, телефонной линии, соединительным линиям ВТСС и специально проложенным кабелям, с использованием направленных микрофонов, размещенных в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных помещениях (непреднамеренное прослушивание).

2) виброакустический – виброакустический канал состоит из тех же элементов, что и акустический: объект сигнала, среда распространения, агент, принимающий данные. Различие состоит в характеристиках среды. Это не воздух, а строительные и иные конструкции, при прохождении по которым акустический канал создает вибрацию, снимаемую при помощи лазерного луча и преобразованную в информацию.

3) акустоэлектрический – акустоэлектрические технические каналы утечки информации возникают вследствии преобразования информативного сигнала из акустического в электрический за счет “микрофонного” эффекта в электрических элементах вспомогательных технических средств и систем. Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающим “микрофонным эффектом”, специальных высокочувствительных низкочастотных усилителей (пассивный акустоэлектрический канал)

4) акустооптический – съем информации осуществляется с плоской поверхно-сти, колеблющейся под действием акустической волны, лазер-ным лучом в ИК-диапазоне, что обеспечивает невидимость его невооруженным глазом. В качестве поверхности, на кото-рую оказывает воздействие акустическая волна, используется внешнее стекло окна. Стекло облучается источником лазерного излучения с внешней стороны, например из окна соседнего дома. На поверхности соприкосновения лазерного луча со стек-лом происходит модуляция лазерного луча акустическими сигналами, генерируемыми в помещении (речь, звуковые ко-лебания работающих технических систем). После отражения от стекла модулированный по амплиту-де и фазе лазерный луч принимается приемником ИК-излучения, преобразуется в электрический сигнал и после соответ-ствующей обработки преобразуется в акустический сигнал, несущий интересующую информацию.

5) параметрический – образование пассивного акустоэлектро-магнитного канала утечки информации связано с наличием в составе некоторых ВТСС высокочастотных генераторов. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным

сигналом. Поэтому этот канал утечки информации часто называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а следовательно, к изменению частоты излучения генератора, то есть к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной ёмкости с воздушным диэлектриком в колебательных контурах гетеродинов.

1.2. Материально-вещественный канал

Данный канал утечки информации возникает за счет неконтролируемого выхода за пределы контролируемой зоны различных материалов и веществ, в которых может содержаться конфиденциальная информация.

Примеры инцидентов и утечек данных по таким каналам:

- Хищение или потеря USB-накопителя.
- Передача физических документов.

1.3. Визуально-оптический канал

Визуально-оптические каналы образуются как оптический путь от объекта конфиденциальных устремлений к злоумышленнику. Для образования визуально-оптических каналов также необходимы определенные пространственные, энергетические и временные условия и соответствующие средства на стороне злоумышленника.

Классификация визуально-оптических каналов утечки информации на рисунке 2.

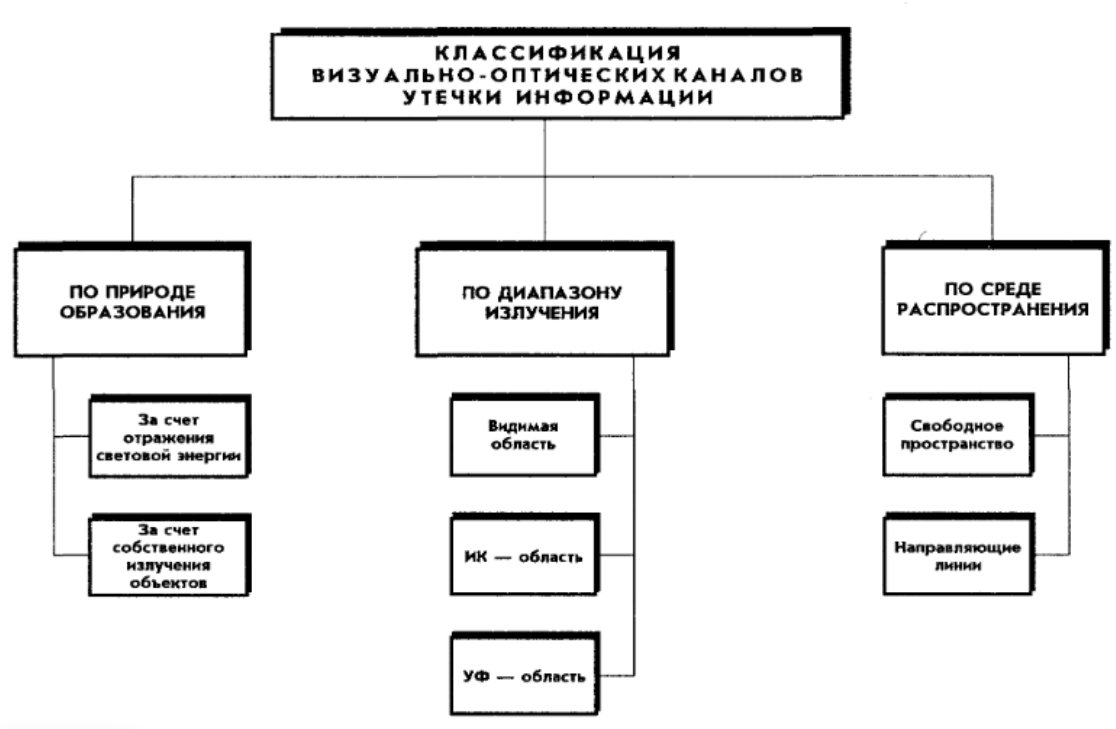


Рисунок 2 – Классификация визуально-оптических каналов утечки информации

Данный канал утечки информации возникает при дистанционном считывании и фиксации информации с различных носителей: например, фотографирование дисплеев мониторов, экранов для демонстрации презентаций, бумажных носителей, аудиозапись переговоров и пр. Непосредственно физического контакта с носителем данных в этом случае не происходит.

Для защиты информации от утечки по этим каналам специалисты по информационной безопасности рекомендуют:

- Ограничивать доступ сотрудников к визуальной информации. В этом помогут специально разработанные политики безопасности.
- Оборудовать помещения, в которых работают с визуальными данными, средствами преграждения или ослабления отраженного света: темными стеклами, шторами, роллетами, ставнями.

- Располагать экраны и другие защищаемые объекты так, чтобы исключить отражение света в сторону посторонних лиц.
- Применять маскировку объектов и носителей информации. Технологий масса — от управления контрастом фона, на котором демонстрируется защищаемая информация, до применения аэрозольных завес и других специальных решений.

1.4. Электромагнитный канал

Электромагнитные каналы утечки информации – это методы перехвата и получения конфиденциальной информации путем анализа электромагнитных излучений, которые генерируются различными устройствами.

Множество устройств, таких как компьютеры, мобильные телефоны, планшеты и другие электронные устройства, генерируют электромагнитные волны в процессе своей работы. Эти волны могут быть перехвачены и анализированы злоумышленниками для получения информации, которая должна быть конфиденциальной.

Примеры электромагнитных каналов утечки информации включают:

- Электромагнитное излучение

Устройства, такие как компьютеры и мониторы, генерируют электромагнитные волны в процессе своей работы. Эти волны могут быть перехвачены и анализированы для получения информации, отображаемой на экране или передаваемой через сеть.

- Электромагнитные импульсы

Некоторые устройства, такие как клавиатуры или считыватели карт, генерируют электромагнитные импульсы при нажатии клавиш или чтении карт. Эти импульсы могут быть перехвачены и анализированы для получения информации, включая вводимые пароли или данные с карты.

- Электромагнитные помехи

Некоторые устройства могут создавать электромагнитные помехи, которые могут быть использованы для перехвата информации. Например, злоумышленник может использовать специальное оборудование для перехвата электромагнитных помех, создаваемых компьютером или другими устройствами, и анализировать их для получения конфиденциальной информации.

Для защиты от электромагнитных каналов утечки информации необходимо применять меры безопасности, такие как использование экранирования, шифрования данных и применение физических мер безопасности, таких как экранные фильтры и защитные экраны.

2 ОБЩАЯ ИНФОРМАЦИЯ О ПРЕДПРИЯТИИ

Наименование предприятия: Общество с ограниченной ответственностью “ВЗГЛЯД” (далее - ООО "ВЗГЛЯД", Общество).

Область деятельности: архитектурное бюро, которое проектирует здания и помещения как для гражданских заказчиков, так и для государства (в том числе для военных нужд).

Структура Общества представлена на Рисунке 3.

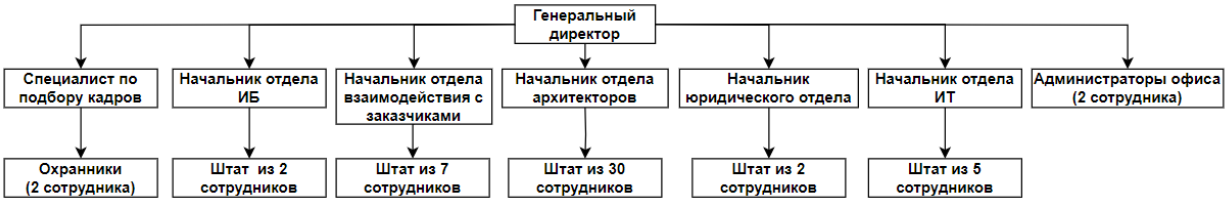


Рисунок 3 – Структура Общества

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

В организации обрабатывается информация конфиденциального характера:

- персональные данные лиц, являющихся и не являющихся работниками Общества;
- сведения, отнесенные к коммерческой тайне организации, включающие в себя деловые секреты, финансово-экономическую, технологическую информацию, технологические секреты организации (ноу-хау), сведения, содержащиеся в служебной документации Общества, кроме официально публикуемых, идеи и разработки, полученные сотрудниками в процессе трудовой деятельности;
- сведения, отнесённые к государственной тайне с уровнем «секретно», включающие в себя обсуждение, разработку и проектирование зданий и помещений для государственных нужд.

Внутренние и внешние информационные потоки внутри Общества представлены на Рисунке 4, который демонстрирует, как данные и информация циркулируют внутри компании и за её пределами.

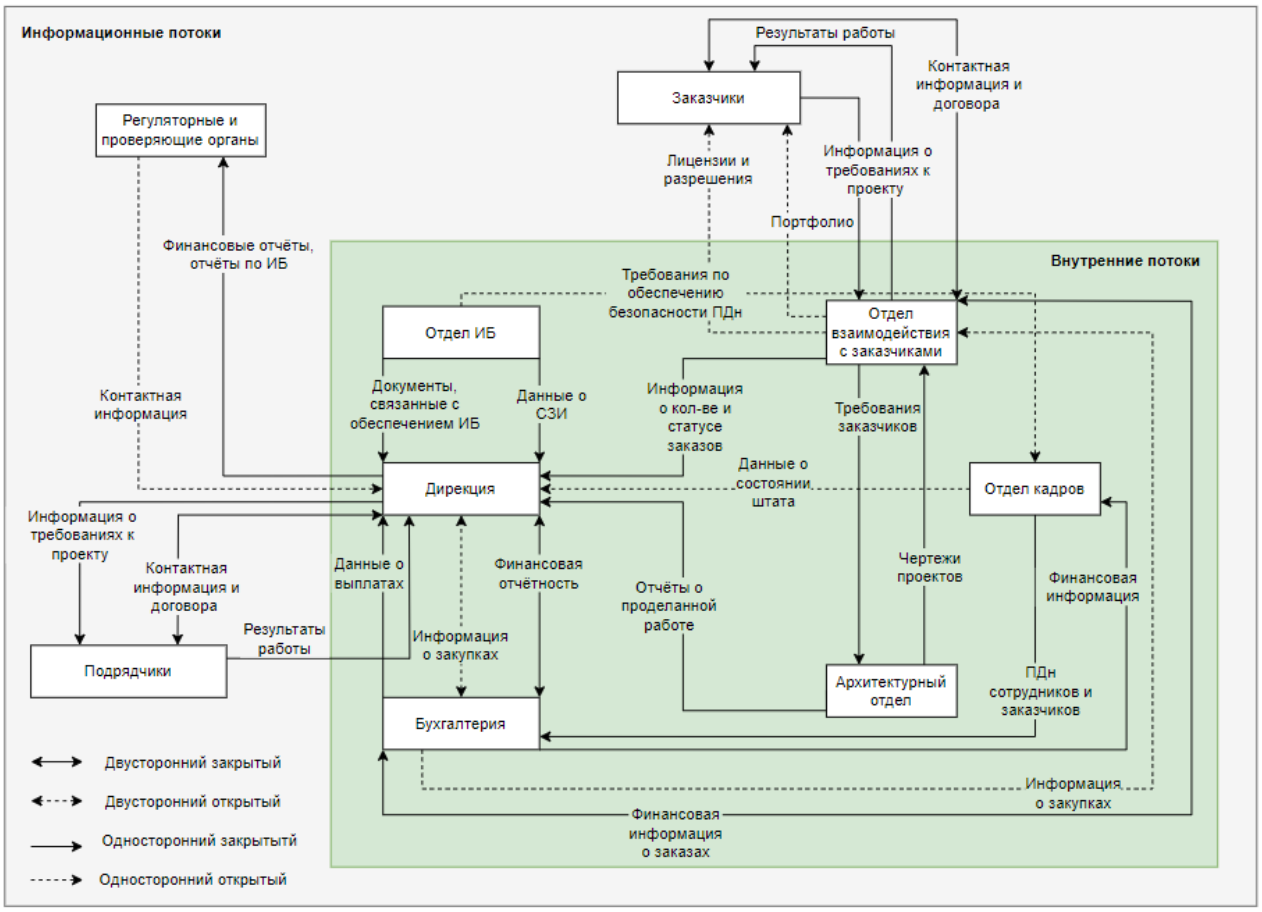


Рисунок 4 – Информационные потоки

3 НОРМАТИВНО-ПРАВОВАЯ БАЗА

Для проектирования инженерно-технической системы защиты информации в Обществе необходимо провести анализ нормативно-правовой базы.

В время работы с любой информацией предприятию необходимо руководствоваться Федеральному закону (далее – ФЗ) №149 "Об информации, информационных технологиях и о защите информации" от 27.07.2006. Данный ФЗ регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий и обеспечении защиты информации.

Так как в Обществе обрабатываются персональные данные лиц, являющихся и не являющихся работниками Общества, то обязательными для выполнения являются следующие нормативно-правовые акты:

1) Федеральный закон №152 "О персональных данных" от 27.07.2006.

Данный ФЗ определяет основные принципы обработки персональных данных и обязанности оператора персональных данных.

«Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных»

2) Приказ ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Данный Приказ включает в себя требование «Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам».

3) Постановление Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

4) Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 "Об утверждении Требований к подтверждению уничтожения персональных данных".

5) Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных".

6) Постановление Правительства Российской Федерации от 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных"

Также в Обществе обрабатывается информация, содержащая государственную тайну с уровнем «секретно». Поэтому актуальны следующие нормативно-правовые акты:

1) Закон РФ "О государственной тайне" от 21.07.1993 №5485-1.

Согласно закону данному ФЗ:

«допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, ***лицензий на проведение работ со сведениями соответствующей степени секретности****»*

«Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

*наличие у них **сертифицированных средств защиты информации**»*

2) Указ Президента РФ от 30.11.1995 N 1203(ред. от 21.09.2011)"Об утверждении Перечня сведений, отнесенных к государственной тайне"

Таким образом, в Обществе обрабатываются сведения, содержащие государственную тайну в военной области:

*«Сведения **о планах строительства** (совершенствования), развитии, численности, боевом составе, боевых возможностях или количестве войск, состоянии боевой готовности войск, состоянии боевого обеспечения, составе дежурных сил (средств) и состоянии их готовности, а также сведения, содержащие анализ военно-политической или оперативной обстановки»*

3) Постановление Правительства РФ от 15.04.1995 №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"

Согласно Постановлению Правительства РФ от 15.04.1995 N 333, пункту 10, специальная экспертиза предприятия проводится путем проверки

выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

4) Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

5) Распоряжение Президента Российской Федерации «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» от 16.04.2005 № 151-рп.

6) Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921–51.

7) Постановление Правительства Российской Федерации «О сертификации средств защиты информации» от 26.06.1995 № 608.

4 АНАЛИЗ ПОМЕЩЕНИЙ ПРЕДПРИЯТИЯ

В данном разделе представлен анализ помещений Общества, который необходимо провести перед разработкой инженерно-технической системы защиты информации.

На рисунке 5 представлен план помещений Общества.

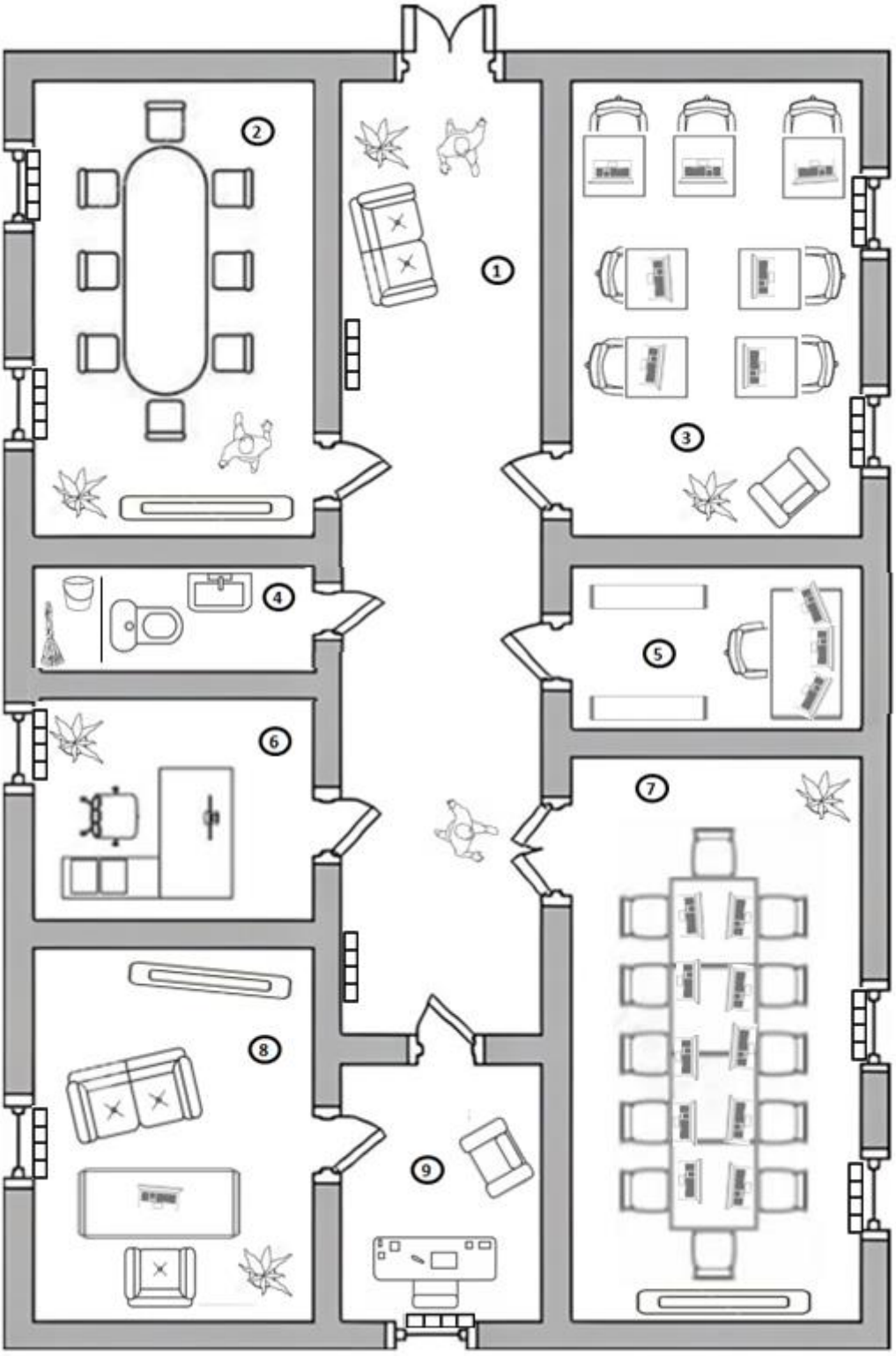
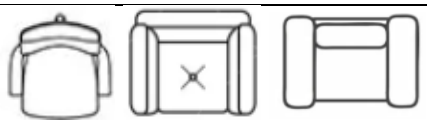
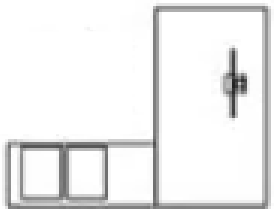
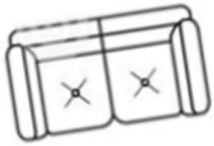
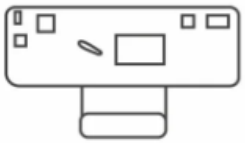
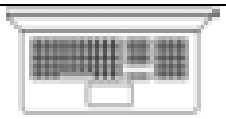
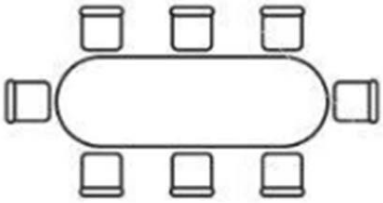
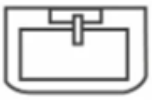
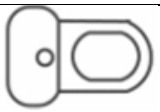
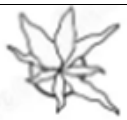
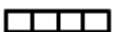


Рисунок 5 – План помещений Общества

В таблице 1 приведено описания всех элементов, изображенных на плане помещения.

Таблица 1 – Описание элементов, изображенных на плане помещения

Обозначение	Наименование
1	Коридор
2	Переговорная
3	Кабинет IT Отдела и ИБ Отдела
4	Уборная
5	Архив
6	Кабинет бухгалтера
7	Кабинет open space
8	Кабинет директора
9	Кабинет секретаря
	Офисные кресла/стулья
	Рабочее место бухгалтера в составе стола, тумбочек и компьютера
	Рабочий стол директора
	Диван в кабинете директора
	Рабочее место секретаря в составе стола, стула и канцелярских принадлежностей
	Рабочее место в помещении архива

	Флипчарт
	Ноутбук
	Стол переговоров
	Раковина
	Унитаз
	Уборочный инвентарь
	Цветок
	Стойка с оборудованием
	Батарея
	Работник Общества

Подробнее изучу помещения Общества по-отдельности:

1) Коридор – общее пространство, представляющее собой проход между кабинетами и имеющее выход на улицу и не имеющее окон. В данном помещении постоянно находится диван, цветок и администратор офиса. Размер помещения 2,5м*14 м.

2) Переговорная – закрытое помещение для переговоров, где обрабатывается информация, составляющая государственную тайну. Стены помещения - 12-и сантиметровая кирпичная кладка. В помещении находится стол переговоров с 8 стульями, 2 окна, 2 батареи, цветок и флипчарт. Размер помещения 7м*4м.

3) Кабинет IT и ИБ Отдела – закрытое помещения, в котором работают сотрудники Общества из IT и ИБ Отделов. В данном помещении

находится 7 рабочих мест (стол + стул), 7 АРМ, диван, цветок, 2 батареи и 2 окна. Размер помещения 7м*4м.

4) Уборная – открытое помещение, которое не имеет окон и батарей. Уборочный инвентарь ширмой отделён от санузла. Размер помещения 2м*4м

5) Архив – закрытое помещение без окон, в котором хранятся чертежи и другая информация, не составляющая государственную тайну. В помещении находятся стойки с документами, 3 АРМ, стол и кресло. В помещении постоянно находится архивариус. Размер помещения 3 м*4м.

6) Кабинет бухгалтера – закрытый кабинет для работы бухгалтера. В кабинете установлены рабочий стол, тумбочки, кресло, цветок и 1 окно и 1 батарея. Размер помещения 4м*4м.

7) Кабинет open space – открытый кабинет для работы сотрудников. В помещении находится 12 рабочих мест, цветок, флипчарт, 2 окна и 2 батареи. Размер помещения 8м*4м.

8) Кабинет директора – закрытый кабинет, в котором работает директор. В этом кабинете могут проводиться переговоры или обрабатываться информация, составляющая государственную тайну. Стены помещения – 12-и сантиметровая кирпичная кладка. В помещении находится стол, кресло, диван, цветок, флипчат, 1 окно и 1 батарея. Размер помещения 5м*4м.

9) Кабинет секретаря – открытый кабинет для работы секретаря. В кабинете находится стол, кресло, диван, 1 окно и 1 батарея. Размер помещения 4м*2,5м.

Помещения расположены на втором этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Окна 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 и внутренние перегородки железобетонные, толщиной не менее 10 см (за исключением переговорной и кабинета директора). Часть внутренних перегородок железобетонные, толщиной не менее 5 см, другая часть сделана из звукоизоляционного гипсокартона.

Таким образом, для данных помещений актуальны технические каналы утечки информации в соответствии с Таблицей 2.

Таблица 2 – Актуальные технические каналы утечки информации

Помещение\ каналы утечки	Акустический	Виброакустический	Материально-вещественный	Визуально-оптический	Электромагнитный
1	-	-	-	-	-

2	+	+	+	+	+
3	+	-	+	+	+
4	-	-	-	-	-
5	+	-	+	+	+
6	-	-	+	+	-
7	-	-	-	+	-
8	+	+	+	+	+
9	-	-	-	+	-

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

5 АНАЛИЗ РЫНКА ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты информации (СЗИ), приведенными в Таблице 3.

Таблица 3 – Необходимые СЗИ

Канал	Источник	Пассивная защита	Активная защита
Акустический (акустоэлектрический и виброакустический)	Открытые окна, двери, проводка, вентиляция	Звукоизоляция, фильтры для сетей электропитания	устройства акустического и вибрационного зашумления, блокираторы сотовой связи
Визуально-оптический	Окна, двери	Жалюзи / шторы на окнах, тонирующие пленки на окна и АРМ	бликующие устройства
Электромагнитный	Розетки, АРМы, бытовая техника, линии связи	Фильтры для сетей электропитания	устройства электромагнитного зашумления

Далее мною будут рассмотрены средства защиты для каждого канала, предлагаемые на рынке.

5.1. Защита акустического канала

Методы защиты акустического канала утечки информации разделяются на пассивные и активные. Пассивные методы направлены на ослабление непосредственных акустических сигналов, циркулирующих в помещении, а также продуктов электроакустических преобразований в ВТСС, ОТСС и соединяющих цепях. Активные методы предусматривают создание маскирующих помех и подавление/уничтожение технических средств акустической разведки.

Основным пассивным методом защиты акустической (речевой) информации является звукоизоляция. Звукоизоляция локализует источники излучения в замкнутом пространстве с целью снижения до предела

отношения сигнал/шум до предела, исключающего или значительно затрудняющего съем акустической информации.

При проектировании выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;

в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;

потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками из таких материалов как резина, пробка, ДВП, МВП и т.п.

В любом помещении наиболее уязвимыми с точки зрения акустической разведки являются двери и окна. Оконные стекла сильно вибрируют под давлением акустической волны, поэтому целесообразно отделить их от рам резиновыми прокладками. По этой же причине лучше применить тройное или хотя бы двойное остекление на двух рамах, закрепленных в отдельных коробах. При этом на внешней раме установить сближенные стекла, а между коробками - звукопоглощающий материал.

Двери обладают существенно меньшими по сравнению с другими ограждающими конструкциями поверхностными плотностями полотен и трудно уплотняемыми зазорами и щелями. Таким образом, стандартная дверь очень плохо защищена, поэтому следует применять двери с повышенной звукоизоляцией или оборудовать защищаемые помещения двойными дверями.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие

отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, прокладок, глушителей, вязкоупругих заполнителей и т.д.

Также одним из наиболее уязвимых мест с точки зрения утечки акустической речевой информации является система вентиляции, так как в ней у звука почти нет преград при распространении. Для затруднения съема информации злоумышленником можно в разрыв воздуховода устанавливать мягкие вставки из плотной ткани или резины.

Для активной защиты требуется сгенерировать в среде распространения сильный помеховый сигнал, который невозможно доступными злоумышленнику техническими средствами отфильтровать от информационного. Естественные помехи, связанные с работой систем ЖКХ, снижают уровень разборчивости сигнала, но к ним необходимо присоединить имеющие техническое происхождение. Анализ таких устройств представлен в Таблице 4.

Таблица 4 – Сравнение устройств защиты акустического канала

Наименование	Описание	Состав	Стоимость
Соната «АВ» модель 4Б	Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам. Первым системообразующим признаком Изделия “Соната-АВ” модель 4Б является построение по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели). Основным положительным следствием такого построения является потенциально более высокая стойкость защиты речевой информации вследствие статистической независимости возбуждения маскирующего шума во всех точках. Вторым инновационным системообразующим признаком Изделия “Соната-АВ” модель 4Б является "интеллектуальность" ее элементов и	Комплекс виброакустической защиты помещения - это комплект, состоящий из устройств СВ-4Б, СА-4Б, Соната ИП-4.3, Соната-ДУ-4.3 и набора креплений для установки.	44 200 р.

	использование проводной линии, связывающей источник электропитания с другими для обмена информацией. Основным положительным следствием такого нововведения является: а) возможность построения системы автоматического контроля всех элементов Изделия “Соната-АВ” модель 4Б при минимально возможной стоимости оборудования и монтажа; б) снижение трудозатрат на конфигурирование и тестирование системы при инсталляции и контроле как следствие возможности адресного управления режимом работы каждого элемента системы; в) возможность изменения настроек генераторов-излучателей "на лету" и, как следствие – возможность построения адаптивной ("многопрофильной") системы виброакустической защиты, обеспечивающей выполнение требований по защищенности при различных вариантах использования помещения ("один в кабинете", "переговоры без звукоусиления", "аппаратура звукоусиления включена"); г) снижение затрат на создание единого комплекса ТСЗИ, т.к. единая линия связи и электропитания для генераторов-излучателей одновременно может использоваться в этом же качестве для других элементов комплекса. - Обладает Сертификатом ФСТЭК. - Диапазон рабочих частот (Гц): 175 - 11 200		
БУРАН	Система акустических и виброакустических помех БУРАН является средством активной акустической и вибрационной защиты акустической речевой информации типа А. Система защиты речевой информации БУРАН обеспечивает: высокое качество шумовой помехи за счет использования аналогового задающего генератора на базе шумодиода; частотную коррекцию спектра помехового сигнала каждого канала; мониторинг уровня нагрузки каналов как в ходе настройки системы, так и в ходе эксплуатации; собственную защиту от утечки информации за счет электроакустических преобразований, паразитной генерации и модуляции речевым сигналом; контроль аварийных ситуаций и визуально-звуковую сигнализацию при отключении одного и более излучателей, коротком замыкании в канале помех, неисправности собственной системы вибрационного	Виброакустический генератор «Буран» - 60 000 руб.; виброакустический генератор «Буран» с возможностью дистанционной автоматической настройки - 80 000 руб.; вибропреобразователь для стен «Молот» с креплением – 4 300 руб.; вибропреобразователь для коммуникаций «Серп-Т» с креплением — 4 300 руб.; вибропреобразователь для рам «Серп-Р» с креплением — 4 300 руб.;	81 000 р.

	зашумления; учет времени наработки под нагрузкой в часах и минутах; защиту от несанкционированного изменения настроек. Основные конкурентные преимущества системы акустических и виброакустических помех БУРАН: число помеховых каналов - три (виброакустических - 2, акустических - 1); возможность подключения большого числа преобразователей - до 50 шт. (виброакустических - до 40 шт., акустических - до 10 шт.); прецизионная система параллельного контроля линий подключения преобразователей; вывод информации о состоянии работы системы на жидкокристаллический индикатор; встроенная перестраиваемая система активной защиты информации от утечки по техническим каналам с программным управлением; оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки; возможность дистанционного включения системы по проводному каналу. - Обладает Сертификатом ФСТЭК. - Диапазон рабочих частот (Гц): 100 - 11 200	вибропреобразователь для окон «Копейка» (пьезоэлектрический) — 3 500 руб.; вибропреобразователь для окон «Копейка-М» (электродинамический) — 4 300 руб.; быстросъемное крепление на раму окна (для виброизлучателей "Копейка", "Копейка-М") — 500 руб.; вибропреобразователь для зашумляемого экрана «Копейка-ЛМ» (электродинамический) — 4 300 руб.; преобразователь акустический «Рупор» – 4 000 руб.; размыкатель аналоговых телефонных линий "Буран-К1" - 5 800 руб.; размыкатель линий оповещения и сигнализации.	
БАРОН 2	Для противодействия техническим средствам перехвата речевой информации (стетоскопы, направленные и лазерные микрофоны, выносные микрофоны) по виброакустическим каналам (наводки речевого сигнала на стены, пол, потолок помещений, окна, трубы отопления, вентиляционные короба и воздушная звуковая волна). Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха. Полностью цифровое управление. Интеллектуальное меню, гибкая система конфигурирования. Возможность формирования помехового сигнала от различных внутренних и внешних	Базовый комплект поставки изделия включает: Виброгенератор «Барон 2». Фонемный клонер. Компакт-диск с программным обеспечением. Выносные радиоприемники – 2 шт. (дополнительная опция). Модуль дистанционного управления по радиоканалу. Пульт дистанционного управления по радиоканалу. Сетевой шнур. Техническое описание и	35 000 р.

	источников и их комбинаций. Внутренние источники - генератор шума, три независимых радиоприемника, фонемный клонер, предназначенный для синтеза речеподобных, оптимизированных для защиты речевой информации конкретных лиц помех путем клонирования основных фонемных составляющих их речи. За счет их микширования значительно уменьшается вероятность очистки зашумленного сигнала. Кроме того, наличие линейного входа позволяет подключать к комплексу источники специального помехового сигнала повышенной эффективности. Каждый канал прибора имеет собственный независимый генератор шума аналогового типа, что позволяет исключить возможность компенсации помехового сигнала средствами перехвата речевой информации за счет специальной обработки, в том числе и корреляционными методами при многоканальном съеме несколькими датчиками. В комплект могут входить до 3-х радиоприемных устройства FM диапазона (два внешних, одно встроенное), каждое из которых имеет возможность перестраиваться по 2 фиксированным частотам со случайным законом продолжительности настройки на каждую частоту. Поэтому с помощью прибора возможно формирование речеподобной помехи, состоящей из смеси сигналов до 6 радиовещательных станций. Одним прибором можно защитить помещения большой площади различного назначения (конференц-залы и т.п.). - Обладает Сертификатом ФСТЭК. - Диапазон рабочих частот (Гц): 60 – 16 000	инструкция по эксплуатации.	

По результатам анализа в качестве устройства акустического зашумления была выбрана система Соната «АВ» модель 4Б со средней ценой, так как имеет возможность подключения к одному питающему шлейфу и индивидуальную регулировку интегрального уровня и корректировку спектра каждого генератора.

А в качестве блокиратора сотовой связи был выбран Аллигатор 80 ЕГЭ, поскольку он ничем не уступает по функционалу, но имеет меньшую стоимость.

5.2. Защита визуально-оптического канала

Защитой информации от утечки по визуально-оптическому каналу называют комплекс мероприятий, полностью исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения света. Самым привычным для человека носителем информации об объектах является видимое человеческим глазом излучение. С помощью зрения человек получает наибольший объем информации.

Плёнка антишпион для мониторов

Плёнка предназначена для скрытия информации при работе за компьютером. Её использование не позволит злоумышленникам подглядеть информацию. Цена за такую плёнку может варьироваться от 1000 до 4000 рублей за 1 штуку.

Окна с отражающим покрытием

Это заполнение для пластиковых окон с зеркально-отражающим напылением. Выполняет функцию приватности – случайные прохожие не смогут увидеть, что происходит внутри помещения. Такое окно, например, можно поставить в переговорную. Цена за такое окно начинается от 5000 рублей и зависит в основном от размера окна.

5.3. Защита электромагнитного канала

Защита информации от утечки по электромагнитным каналам — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

В качестве пассивной защиты применяется установке фильтров для сетей электропитания во всех помещениях. В качестве пассивной защиты помещений используются электромагнитные экраны, препятствующие прохождению волн.

В качестве активной защиты применяется создание в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. Анализ данных устройств приведён в Таблице 65

Таблица 5 – Сравнение устройств защиты электрического канала

Наименование	Описание	Стоимость
ЛГШ-221	Сетевой генератор шума «ЛГШ-221» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок путем формирования маскирующих шумоподобных помех. Изделие «ЛГШ-221» соответствует типу «Б» - средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны. Изделие «ЛГШ-221» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-221» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Конструкция Изделия «ЛГШ-221» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним. Изделие «ЛГШ-221» имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».	36 500 р.
Соната-РС3	Генератор шума СОНАТА-РС3 – средство активной защиты конфиденциальной информации от утечки по проводам электросети. Это устройство предназначено для использования в помещениях, в которых на электронно-вычислительных машинах обрабатываются данные, являющиеся коммерческой либо государственной тайной. Благодаря наличию у данного оборудования сертификата ФСТЭК, оно может эксплуатироваться в выделенных помещениях любой категории.	32 400 р.

	СОНАТА-РС3 после подключения к электросети генерирует электромагнитные шумы – наводки на провода электропитания и заземления. Такие помехи поглощают конфиденциальные данные, содержащиеся в побочных излучениях, и делают невозможным их похищение. Средство активной защиты информации СОНАТА-РС3 обладает следующими эксплуатационными характеристиками: - возможность регулирования уровня излучаемых электромагнитных шумов; - возможность блокировки прибора от несанкционированного доступа; - световой и звуковой индикаторы работы и контроля уровня излучения; - совместимость с проводными пультами ДУ линейки СОНАТА.	
Генератор шума SEL SP-44	Двухканальный генератор зашумления SEL SP-44 предназначен для активной защиты цепей энергопитания от съема информации злоумышленниками. Принцип работы генератора заключается в создании высоко- или низкочастотных шумов, которые наводятся на провода питания и заземления. Эти наводки - шумовые помехи, надежно маскирующие все сигналы и делающие невозможным похищение информации. - Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3-1 категорий - 2-канальный цифровой генератор шумовых сигналов в диапазоне 10кГц-400МГц - Активная защита конфиденциальных сведений от утечки по проводам электропитания - 2 независимых друг от друга формирователей шума - Возможность регулировки уровня ВЧ и НЧ шумов - Световая и текстовая индикация работы - Звуковой сигнал при переходе в аварийный режим - Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе.	26 000 р.

По совокупности характеристик в качестве средства защиты электрического, акустоэлектрического и электромагнитного каналов утечки информации выбран генератор шума «Соната-РС3».

5.4. Защита от ПЭМИН

При работе самых различных устройств (например, вычислительной техники) могут появляться сигналы ПЭМИН (побочные электромагнитные излучения и наводки), содержащие обрабатываемую информацию конфиденциального характера. Эти сигналы могут быть перехвачены с помощью специальной аппаратуры.

Таблица 6 – Сравнение устройств защиты от ПЭМИН

Наименование	Описание	Стоимость
ПУЛЬСАР	Генератор электромагнитного шума "Пульсар" - инновационное устройство, разработанное для эффективной маскировки и защиты информации от потенциальных угроз, связанных с электромагнитными излучениями и наводками (ПЭМИН). Рассчитан на использование в сфере компьютерных технологий и обеспечивает надежную защиту ограниченного доступа к конфиденциальным данным, включая государственную тайну всех категорий, даже вплоть до грифа "Совершенно секретно". - Имеет сертификаты ФСТЭК и Минобороны. - Имеет диапазоны частот от 10 кГц до 6 ГГц - 2 съемные антенны, счетчик наработки - Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук)	25 600 р.
Соната-Р3.1	Средство активной защиты информации "Соната-Р3.1", предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации. ПЭМИН Соната-Р3.1 обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений. Соната-Р3.1 в базовой комплектации конструктивно выполнена в виде моноблока с сетевым шнуром. В моноблоке находится регулируемый генератор шума, интегрированный со сверхширокополосной антенной и адаптером ввода шумового тока в сеть электропитания. Производитель, по желанию заказчика, может комплектовать изделие следующими дополнительными опциями:	42 000 р.

	- дополнительная антенна "Веер"; - элементы крепления и фиксации (кронштейны, кольца монтажные); - пульт управления "Соната-ДУ4.3" в комплексе с блоком питания "Соната-ИП4.х"; - пульт управления "Соната-ДУ4.4". Дополнительная антенная система "Веер" применяется для повышения уровней электромагнитного поля шума (ЭМПШ) в диапазоне частот 0,01…200 МГц. Антенна "Веер". Приобретается отдельно и устанавливается покупателем самостоятельно при необходимости.	
ЛГШ-503	Генератор белого шума ЛГШ-503 соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты. Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Конструкция генератора обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина». Комплектация: Генератор ЛГШ 503 - 1шт. Руководство по эксплуатации - 1шт. Паспорт - 1шт. Вилка кабельная ДУ - 1шт. Упаковка 1шт Знак соответствия - 1шт. Копия сертификата соответствия ФСТЭК России - 1шт.	45 000 р.

По совокупности характеристик в качестве средства защиты от ПЭМИН выбран «Соната-Р3.1».

6 РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЯ

На основе результатов анализа плана помещения предприятия и результатов анализа рынка инженерно-технических средств защиты информации была разработана инженерно-техническая система защиты информации для Общества (Рисунок 6).

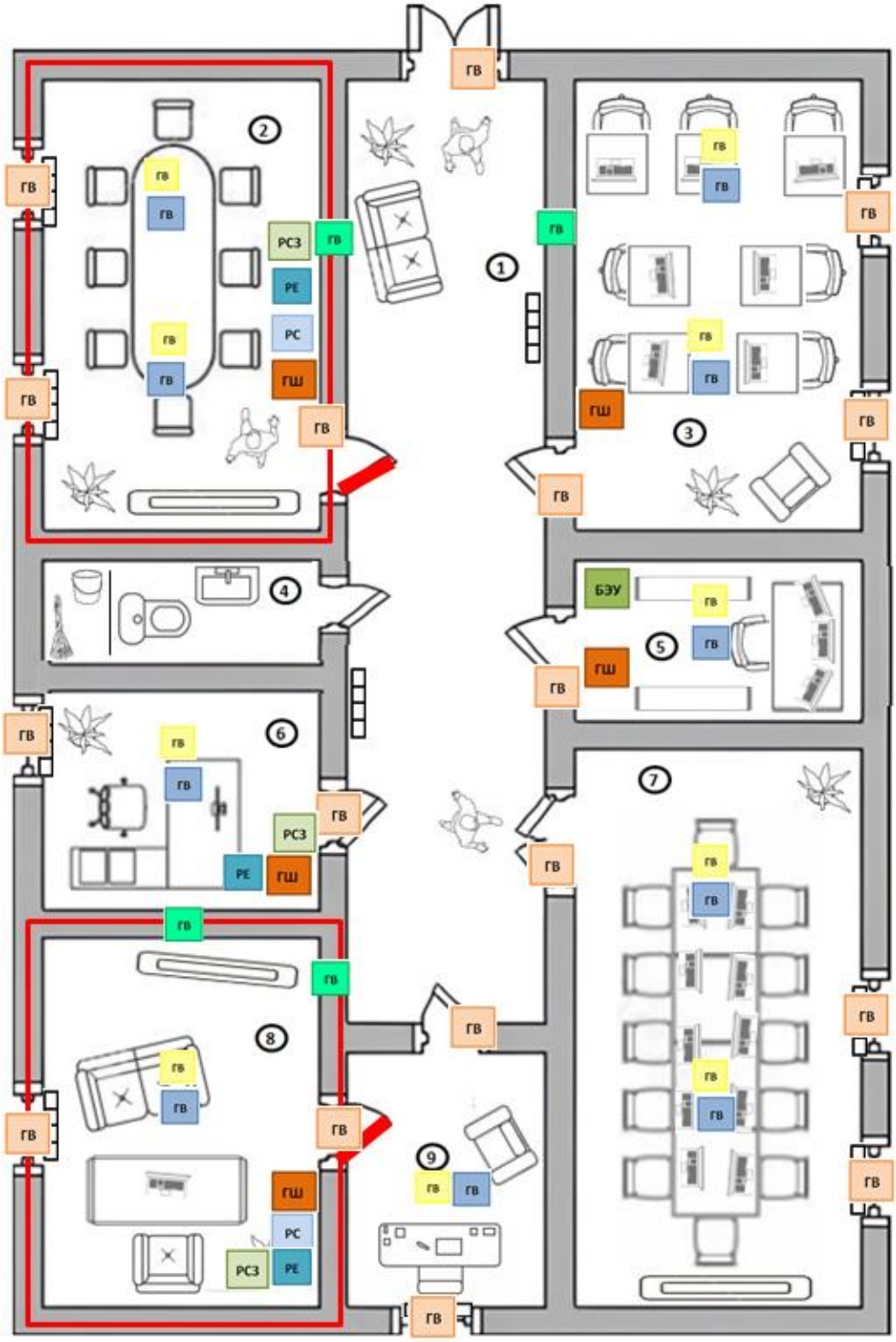
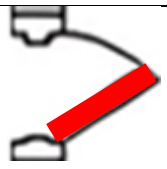


Рисунок 8 – Схема установки устройств на плане

Условные обозначения представлены в Таблице 8.

Таблица 8 – Условные обозначения

Обозначение	Наименование
БЭУ	«Соната-ИП4.3» блок электропитания и управления
ГВ	«Соната-СВ-4Б1» генератор-акустоизлучатель
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна, батареи)
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (стены)
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок)
ГШ	«Соната-Р3.1» генератор шума (от ПЭМИН)
РС	Размыкатель слаботочных линий Соната-ВК4.2
РЕ	Размыкатель линий Ethernet Соната-ВК4.3
РСЗ	"Соната-РСЗ" Средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания
	Отделка помещений звукоизолирующим материалом
	Дверь звукоизолирующая

ЗАКЛЮЧЕНИЕ

В ходе курсовой работы анализ технических каналов утечки информации, анализ рынка средств защиты информации, а также разработана инженерно-техническая система защиты для Общества.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. О государственной тайне: Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) // Собрание Законодательства Российской Федерации.
2. Постановление Правительства РФ "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 15.04.1995 № 333 // Официальный интернет-портал правовой информации
3. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — No3 (107). — С. 69–72. — URL: https://moluch.ru/archive/107/25842/ (дата обращения: 11.12.2023).
4. Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. // Защита информации от утечки потехническим каналам. URL: learn.urfu.ru/resource/index/data/resource_id/40977/revision_id/ (дата обращения: 11.12.2023).