

**Министерство науки и высшего образования Российской Федерации
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 защиты
информации на предприятии

Вариант 97

Выполнил:



Рахимов Э. Р.,

студент группы N34501

Проверил преподаватель:

Попов И. Ю., доцент ФБИТ

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Рахимов Эмиль Русланович

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, 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 Разработать систему инженерно-технической защиты информации на предприятии

Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
2. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент

19.12.2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Рахимов Эмиль Русланович

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, 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
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	25.11.2023	25.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	30.11.2023	02.12.2023	
4	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель _____

(Подпись, дата)

Студент _____

19.12.2023

(Подпись, дата)

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

Студент Рахимов Эмиль Русланович

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, 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

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Целью работы является повышения уровня безопасности рассматриваемого помещения. Задачами является проведение анализа безопасности помещения, оценка возможных каналов утечки информации, а также определение мер по укреплению как пассивных, так и активных способов защиты информации.

**2. Характер
работы**

- ☐ Расчет ☒ Конструирование
☐ Моделирование Другое _____

Содержание работы

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

3. Выводы

По итогам исследования были выделены универсальные методы предотвращения утечки информации по техническим каналам на предприятии. В условиях постоянно эволюционирующих угроз кибер- и физической безопасности стратегии защиты требуют применения современных способов предотвращения утечек информации и постоянного их улучшения. Важную роль в предотвращении утечки играет не только пассивная защита, но и активная. Успешная защита требует не только технологических решений, но и формирования культуры безопасности внутри организации через обучение сотрудников и повышение их

ответственности. Сбалансированный и комплексный подход к безопасности остается неотъемлемой

частью эффективных стратегий в современном информационном обществе.

Руководитель _____

Студент _____



(Подпись, дата)

19.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

Введение	7
1 Организационная структура предприятия	9
1.1 Анализ технических каналов утечки информации	9
1.2 Информационные потоки.....	14
1.3 Перечень руководящих документов	15
1.4 Структура информационных потоков на предприятии.....	18
2 Обоснование защиты информации.....	19
3 Анализ защищаемых помещений	22
3.1 Схема помещения.....	22
3.2 Описание помещений	25
3.3 Анализ возможных каналов утечки информации.....	27
4 Анализ рынка технических средств	28
4.1 Выбор средств защиты	28
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	29
4.3 Защита от утечки информации по (вибро-) акустическим каналам ...	31
4.4 Защита от ПЭМИН.....	34
4.5 Защита от утечек информации по оптическим каналам	36
5 Описание расстановки технических средств.....	37
Заключение.....	42
Список использованных источников.....	43

ВВЕДЕНИЕ

Средства защиты информации (СЗИ) выполняют функцию защиты данных в информационных системах, которые включают в себя хранилища информации в базах данных, информационные технологии для её обработки, а также соответствующие технические устройства. Эти средства предотвращают несанкционированный доступ злоумышленников к ресурсам и данным предприятия, тем самым уменьшая риск несанкционированных утечек, потерь, искажений, уничтожения, копирования и блокирования информации. Это также способствует предотвращению возможных экономических, репутационных и других видов ущерба для предприятия. Разработка эффективного комплекса мер по решению этой задачи представляет собой одну из наиболее актуальных проблем современности. Технические средства защиты информации играют важную роль в обеспечении режима конфиденциальности на предприятии.

В данной работе рассматривается процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «совершенно секретно» на объекте информатизации. Объект защиты включает в себя десять помещений, представляя собой офис предприятия с переговорной, кабинетом директора, серверной, одним санузелом, четырьмя кабинетами отдела разработки, главным холлом, серверной и кухней.

Работа разбита на пять глав. Первая глава посвящена анализу технических каналов для возможной утечки информации. Во второй главе представлен перечень управляющих документов, в третьей произведен анализ защищаемых помещений с учетом возможных рисков утечек информации и необходимых технических средств для обеспечения защиты. Четвертая глава включает в себя анализ рынка технических средств защиты информации различных категорий, а пятая глава посвящена разработке схемы размещения выбранных технических средств

в защищаемых помещениях.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Анализ технических каналов утечки информации

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Согласно теме курсовой работы, рассматриваться будет только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала,

представляющего собой носитель с информацией от её источника.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Информация от источника поступает на вход канала на языке источника, поэтому полученную информацию передатчик преобразует в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.



Рисунок 2 – Классификация технических каналов утечки информации

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Акустические ТКУИ в свою очередь делятся на акустоэлектрическом, виброакустическом и акустические.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей

используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с

функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействуют на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещении есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технические устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве

вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

1.2 Информационные потоки

Информационный поток — это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления, анализа и контроля логистических операций. Они играют ключевую роль в функционировании предприятия, их правильное управление и защита существенны для обеспечения конфиденциальности, целостности и доступности информации. Они могут существовать в виде бумажных, электронных документов (носителей), звука, символов и сигналов.

Информационные потоки могут быть классифицированы по различным критериям. Согласно цели данной работы информационные потоки будут разделены на две основные категории: открытые и закрытые.

Открытые информационные потоки представляют собой те, которые доступны сотрудникам и другим заинтересованным сторонам в пределах предприятия без специальных ограничений. Они включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Примеры открытых информационных потоков включают в себя общие отчеты, обновления проектов и новости

компании. Открытые информационные потоки способствуют эффективному внутреннему обмену информацией и содействуют открытости и прозрачности внутри организации.

Закрытые информационные потоки содержат конфиденциальную, чувствительную информацию, которая требует высокого уровня защиты. Эти потоки могут включать в себя финансовые данные, персональные записи, интеллектуальную собственность и другие данные, которые, если попадут в неправильные руки, могут нанести ущерб предприятию.

Защита закрытых информационных потоков включает в себя установление строгих политик доступа, шифрование данных, мониторинг активности и другие меры безопасности.

1.3 Перечень руководящих документов

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212;
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108;
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального

характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- инструкция №0126–87;
- 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;
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;
- «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. №333;
- «О внесении дополнения в Положение 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 30 апреля 1997 г. №513;
- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;
- «О сертификации средств защиты информации» от 26 июня 1995

г, №608.

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;
- методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;
- временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
- временный порядок аттестации объектов информатизации по требованиям безопасности информации;
- руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;
- 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;
- руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

– руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;

– руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования;

– руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;

– руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Также, необходимо обратить внимания на законы Российской Федерации:

- «О государственной тайне» от 21 июля 1993 г. №5151–1;
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ;
- «О безопасности» от 5 марта 1992 г. №2446–1;
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1;
- «О связи» от 16 февраля 1995 г. №15-ФЗ;
- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

1.4 Структура информационных потоков на предприятии

На рисунке 3 голубым цветом обозначены открытые потоки, а оранжевым цветом – закрытые потоки.

К информации, передающейся по открытым потокам, относятся бухгалтерская и финансовая отчетность, налоговые сведения.

К защищаемой информации, передающейся по закрытым потокам,

относятся персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна и сведения о разрабатываемом программном продукте (программный код, назначение и т. д.).

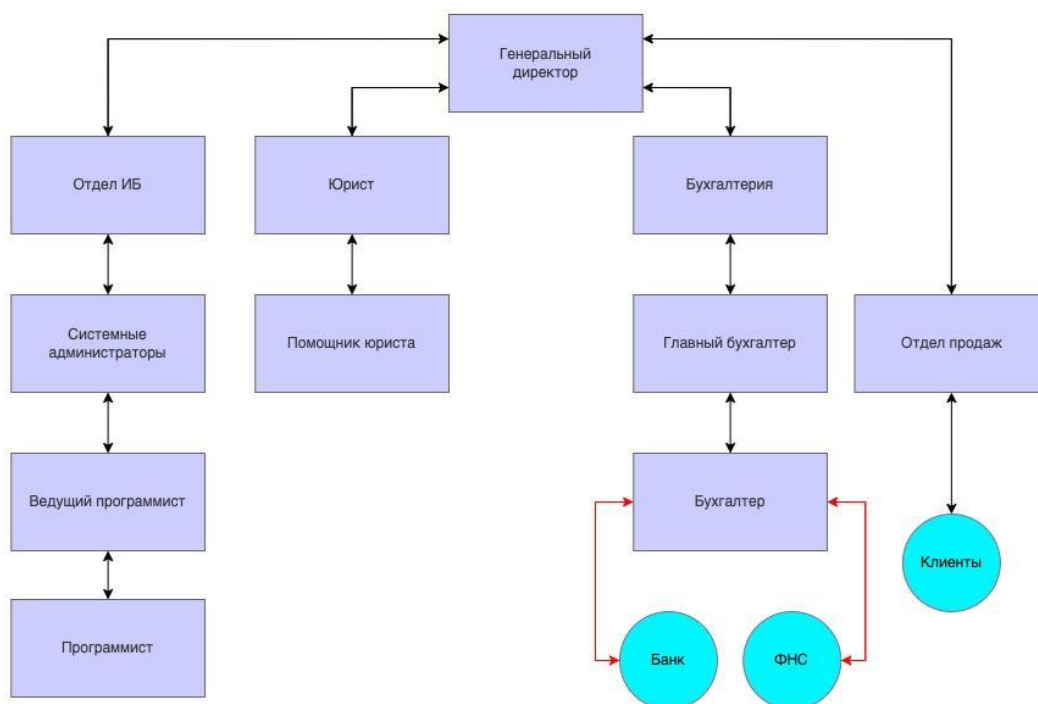


Рисунок 3 – Схема информационных потоков на предприятии

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери,

обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 сантиметров. Дверь устанавливается на металлический каркас;

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;

3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем эта- же, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене;

4. Все режимные помещения оборудуются аварийным освещением;

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

Согласно Руководящему документу Государственной технической комиссией 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» (таблица 1).

Таблица 1 – Классы защищенности автоматизированных систем

<p>Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
<p>Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)</p>	2А	Информация, составляющая гостайну

	2Б	Служебная тайна или персональные данные
--	----	---

Продолжение таблицы 1

Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке 4. В таблице 2 представлены описание обозначений, изображенных на плане.

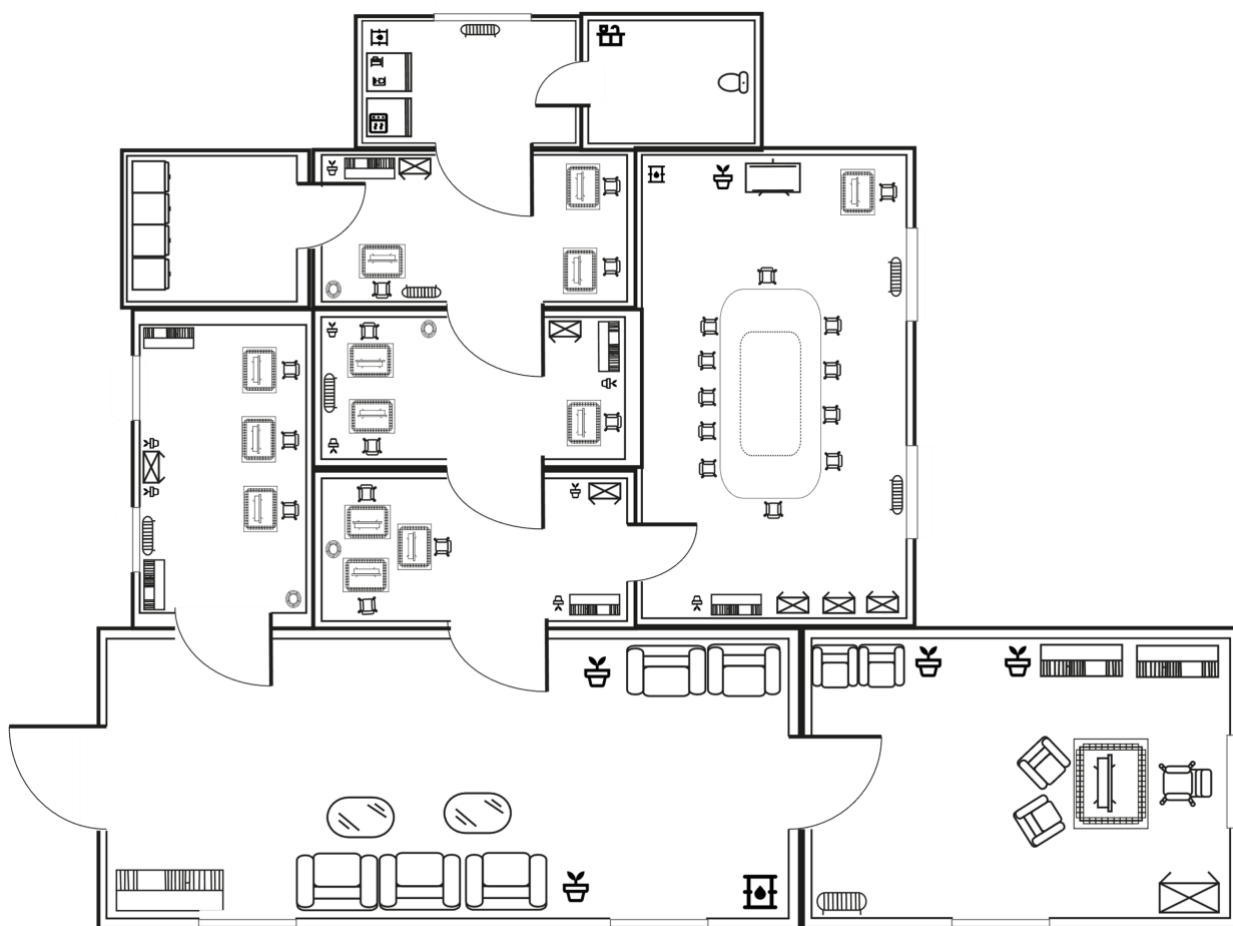


Рисунок 4 – План защищаемого помещения

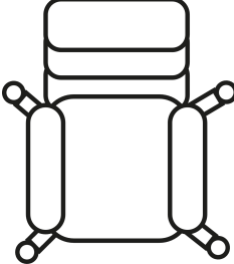
Таблица 2 – Описание обозначений

Обозначение	Описание
	Интерактивная доска с проектором
	Журнальный стол
	Книжная полка
	Комнатное растение
	Компьютер

Продолжение таблицы 2

	Компьютерный стол
	Кофе машина
	Кресло
	Кулер для воды
	Кухонный стол
	Мусорное ведро для бумаги
	Офисный стул
	Радиатор отопления
	Раковины
	СВЧ-печь

Продолжение таблицы 2

	Сервер
	Стол переговоров
	Стул руководителя
	Унитаз
	Чайник
	Шкаф для документов

3.2 Описание помещений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- кабинет директора (15,9 м²);
- переговорная комната (19,2 м²);
- офис 1 (16,8 м²);

- офис 2 (15,6 м²);
- офис 3 (15,6 м²);
- офис 4 (15,6 м²);
- серверная комната (8,4 м²);
- кухня (9,0 м²);
- главный холл (20,4 м²).

Кабинет директора включает в себя: один стул руководителя, два стула, два офисных кресла (совмещенных), один компьютерный стол, два книжных шкафа, один шкаф для документов, один радиатор отопления, два окна и два комнатных растения. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся одиннадцать стульев, один стол для переговоров, один компьютерный стол, один компьютер, три шкафа для документов, одна интерактивная доска с проектором, один кулер для воды, два радиатора отопления, два окна и одно комнатное растение. Переговорная комната оснащена восьмью розетками.

Офис 1, офис 2, офис 3, офис 4 предназначены для сотрудников предприятия.

В офисе 1 стоят три стула, три компьютерных стола, три компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно комнатное растение. В данном помещении находятся шесть розеток.

В офисе 2 есть три стула, три компьютерных стола, три компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления и три комнатных растения. Данное помещение оснащено восьмью розетками.

В офисе 3 находятся три компьютерных стола, три компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги и два комнатных растения. Офис 3 оснащен шестью розетками.

В офисе 4 стоят три стула, три компьютерных стола, три компьютера, два книжных шкафа, один шкаф для документов, одно мусорное ведро для

бумаги, один радиатор отопления, два окна и два комнатных растения. В данном помещении находятся шесть розеток.

В серверной комнате расположены четыре сервера. В данном помещении есть двенадцать розеток.

В кухне есть одно окно, один радиатор отопления, кулер для воды и кухонный стол, на котором находятся одна кофемашина, одна микроволновая печь и один чайник. Данное помещение включает в себя пять розеток.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся три кресла (совмещенных), два кресла (совмещенных), два журнальных стола, книжный шкаф, два комнатных растения и кулер для воды.

Окна помещения выходят в закрытый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 11 см.

3.3 Анализ возможных каналов утечки информации

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы,

например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не перекрывается техническими средствами защиты.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 3. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Электрический Электромагнитны й	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитно го зашумления	Защитные экраны и фильтры для сетей электропитания

Продолжение таблицы 3

Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений
Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов
Визуально- оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Защитные экраны и фильтры для сетей электропитания

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств,

относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 4.

Таблица 4 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума SEL SP-44	26 000	Уровень шума затухания 12–90 дБ. Напряжение 220 В \pm 10% 50 Гц. Диапазон частот 10 кГц – 400 МГц. Количество фаз – 1 с заземлением.	Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3–1 категорий. Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе
Генератор шума ЛГШ-221	36 400	Ток нагрузки – сеть \sim 220 В +10%/-15%, 50 Гц. Напряжение – 220 В. Количество фаз – 1. Потребляемая мощность 10 Вт.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта. Сертифицировано ФСТЭК.
Генератор шума СОНАТА-РС3	32 400	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Напряжение 220 В.	Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)

На основании анализа, проведенного в таблице 4, был выбран генератор

шума ЛГШ-221. Оптимальный вариант по соотношению цена и качество позволяют установить достаточное количество подобных устройств в помещениях. Кроме того, этот выбор был обоснован наличием сертификата ФСТЭК большим ресурсом работы генератора – 27 000 часов.

4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б (таблица 5).

Таблица 5 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175– 11200 Гц. Выходное напряжение В $12,5 \pm$ 0,5. Электропитание сеть ~220 В/50 Гц.	Комплект состоит из блоков электропитания и управления, генераторов- акустоизлучателей, генераторов- вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Камертон–5	46 000	Электропитание от сети. электропитание СВАЗ «Камертон-5» исп.2 осуществляется от сети переменного тока частотой 50 Гц с напряжением от 187 В до 242 В, по отдельным компонентам. Индикация – световая, звуковая, ЖК	Предназначено для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов.
SEL SP-157 Шагренъ	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.

Исходя из анализа, представленного в таблице 5, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее

востребованной и получила множество положительных отзывов.

4.4 Защита от ПЭМИН

Таблица 6 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ 503	44 200	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -26 дБ (мкА/м*$\sqrt{\text{кГц}}$) до 50 дБ(мкВ/м*$\sqrt{\text{кГц}}$).</p> <p>Мощность – 45 Вт.</p>	<p>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.</p> <p>Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>

Продолжение таблицы 6

Модель	Цена, руб.	Характеристики	Особенности
Базовый генератор маскирующих радиопомех ГШ-111Б	39 000	Наличие регулировки уровня шума. Диапазон частот 10 кГц - 1800 МГц. Уровень шума от 0 до - 30 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А.	На задней панели генератора расположены отдельные выходы для подключения магнитной и радиочастотных антенн, а также выход на внешнее устройство наведения шумового сигнала на провода. Интерфейс для управления и контроля ГШ по сети Ethernet 10/100 Мбит/с.
SEL-155 «СОНЕТ»	39 800	Наличие регулировки уровня шума. Диапазон частот от 0,01 до 1800 МГц. Уровень шума до 32 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А. Мощность 30 Вт для управляющего блока.	Сертификат ФСТЭК. Защита речевой информации тип «Б» по 2 классу. Также система предназначена для защиты телефонных линий, линий компьютерных сетей, соединительных линий систем оповещения и сигнализации от утечки по каналу акустоэлектрических преобразований

В качестве средства активной защиты от ПЭМИН был выбран генератор

шума «ЛГШ-503». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

4.5 Защита от утечек информации по оптическим каналам

Для прекращения функционирования оптического канала утечки информации можно применить следующие меры:

- шторы на окна;
- жалюзи;
- тонированные пленки на стеклах.

Шторы – традиционные средства для предотвращения скрытного наблюдения через окна кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты делать не следует. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания.

Наиболее приемлемый вариант защиты – применение жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению – защите от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

Для предотвращения снимков экрана существует свободно распространяемое ПО для ОС Windows – ScreenWings.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума ЛГШ–221;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-503» от ПЭМИН
- жалюзи на семь окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15...25 м² перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей

«Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

В таблице 7 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 7 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума ЛГШ-221	32 800	1	32 800
Генератор шума «ЛГШ- 503»	44 200	1	44 200
Блок электропитания и управления «Соната- ИП4.3»	21 600	1	21 600
Генератор- акустоизлучатель «Соната СА-4Б1»	3 540	18	63 720
Генератор- вибровозбудитель «Соната СА-4Б»	7 440	57	424 080
Рызмыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель линии «Ethernet» «Соната ВК4.1»	6 000	1	6 000

Продолжение таблицы 7

Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	9	44 100
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			913 037

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «ЛГШ-221» и «ЛГШ-503» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 8 приведены описание обозначений устройств.

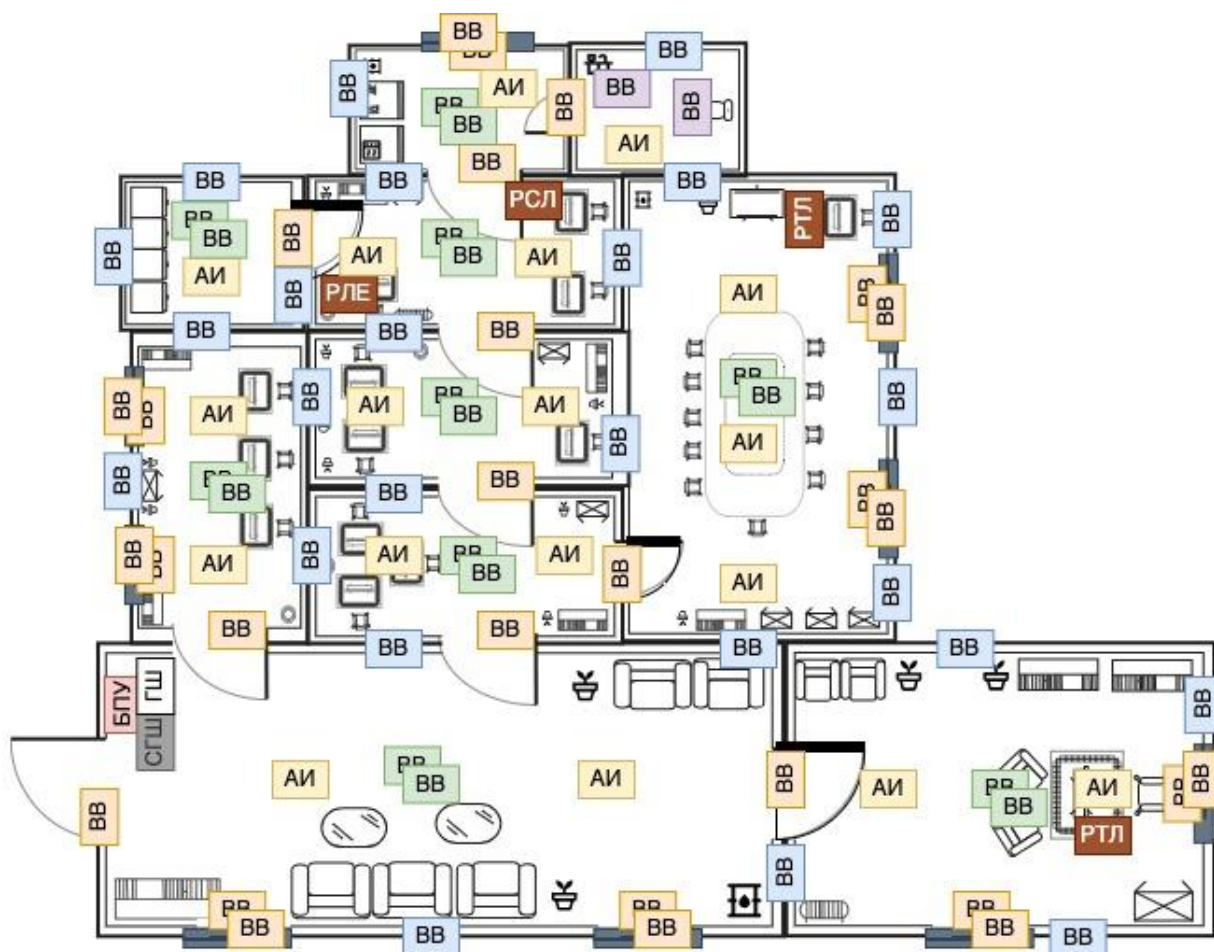

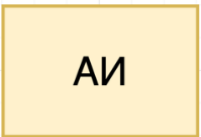
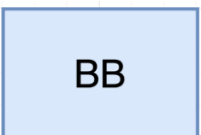


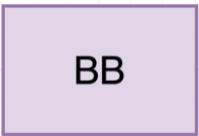

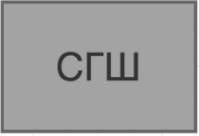

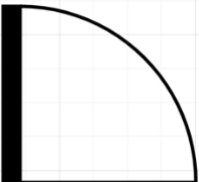



Рисунок 5 – Схема расстановки устройств

Таблица 8 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	18
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	17

Продолжение таблицы 8

Обозначение	Устройство	Количество, шт.
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	18
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	20
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	2
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Сетевой генератор шума «ЛГШ- 221»	1
	Генератор шума «ЛГШ-503»	1
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	9

ЗАКЛЮЧЕНИЕ

В процессе формирования данной курсовой работы был проведен анализ как открытых, так и закрытых потоков информации на предприятии. Осуществлено обоснование необходимости защиты информации, включенной в государственную тайну уровня «совершенно секретно» на данном предприятии. Дополнительно был проведен анализ уровня безопасности помещений, выявлены актуальные каналы утечки информации. На основе проведенного анализа были выбраны соответствующие средства защиты информации, учитывая актуальные данные рынка. Следующим этапом был разработан план размещения технических средств защиты информации, с проведением расчетов стоимости внедрения.

В результате выполненной работы был разработан план по обеспечению защиты помещения от потенциальных каналов утечки информации, включая пути передачи информации через ПЭМИН, а также посредством электрических, акустоэлектрических, электромагнитных, акустических, виброакустических и оптических маршрутов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. 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.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).