

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

**«Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 48»**

Выполнил(а):

Студент группы N34481

Давыдов Степан

Сергеевич

_____ 

Проверил преподаватель:

Попов Илья Юрьевич,

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 Давыдов Степан Сергеевич

(Фамилия И.О.)

Факультет Безопасности Информационной Технологий

Группа N34481

Направление (специальность) 10.03.01 Технологии защиты информации

Руководитель Попов Илья Юрьевич, доцент ФБИТ Университета ИТМО

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

Дисциплина Инженерно-технические средства защиты информации

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

Задание Разработка комплекса инженерно-технической защиты информации в
помещении

Краткие методические указания

Подготовить отчет по курсовой работе

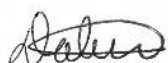
Содержание пояснительной записки

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



19 декабря 2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Давыдов Степан Сергеевич

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34481

Направление (специальность) 10.03.01 Технологии защиты информации

Руководитель Попов Илья Юрьевич, доцент ФБИТ Университета ИТМО

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

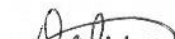
Дисциплина Инженерно-технические средства защиты информации

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 согласования задания	25.09.23	25.09.23	
2	Создание плана КР	28.09.23	28. 09.23	
3	Анализ теоретической составляющей	14.10.23	14.10.23	
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	28.10.23	28.10.23	
5	Защита курсовой работы	19.12.23	19.12.23	

Руководитель

(Подпись, дата)

Студент  19 декабря 2023

(Подпись, дата)

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

Студент Давыдов Степан Сергеевич
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34481

Направление (специальность) 10.03.01 Технологии защиты информации

Руководитель Попов Илья Юрьевич, доцент ФБИТ Университета ИТМО
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

- 1. Цель и задачи работы**
- ☐ Предложены студентом ☐ Сформулированы при участии студента
- ☒ Определены руководителем

Цель: Повышение защищенности рассматриваемого помещения. Задачи: анализ помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты.

- 2. Характер работы**
- ☐ Расчет ☒ Конструирование
- ☐ Моделирование ☐ Другое

3. Содержание работы

В работе представлена нормативно правовая база, анализ защищаемых помещений, анализ и сравнение технических средств защиты информации, план расстановки технических средств

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель _____
(Подпись, дата)

Студент  19 декабря 2023
(Подпись, дата)

СОДЕРЖАНИЕ

Введение	6
1 Анализ технических каналов утечки информации	7
2 Руководящие документы	10
2.1 Законы Российской Федерации	10
2.2 Указы Президента Российской Федерации	10
2.3 Постановления Правительства Российской Федерации	10
2.4 Решения Гостехкомиссии России	11
2.5 Руководящие и нормативно-методические документы Гостехкомиссии	12
3 Структурная модель и анализ защищаемого объекта	15
3.1 Структура организации	15
3.2 Обоснование защиты информации	16
3.3 Описание инженерно-технических показателей объекта	17
4 Анализ и сравнение технических средств защиты информации	22
4.1 Устройства противодействия утечке информации по акустическому и виброакустическому каналам	22
4.2 Устройства противодействия утечке информации по оптическому каналу	23
4.3 Устройства противодействия утечке по электромагнитным и электрическим каналам	23
5 Расстановка выбранных инженерно-технических СЗИ на плане	25
Заключение	27
Список используемой литературы	28

ВВЕДЕНИЕ

Для создания эффективной системы информационной защиты необходимо сначала определить потенциальные и реальные угрозы технического вторжения на защищаемый объект, а также возможные пути несанкционированного доступа и утечки информации.

Эта работа основана на понимании происхождения технических каналов для утечки информации и методов технической разведки. Правильное определение потенциальных угроз на этапе предпроектирования системы защиты позволит выбрать наиболее оптимальные меры и средства защиты.

При обнаружении технических путей утечки информации важно рассмотреть все элементы защиты, включая основное оборудование для обработки информации, связующие линии, устройства коммутации, системы электропитания, вентиляции и другие.

Помимо основного оборудования, связанного с обработкой и передачей конфиденциальной информации, необходимо учитывать вспомогательные технические средства и системы (ВТСС), такие как средства связи, системы безопасности, электрические приборы и другие. Особое внимание следует уделить вспомогательным средствам, имеющим связи за пределами контролируемой зоны.

При оценке возможных путей утечки информации следует обратить внимание на вспомогательные средства с выходами за пределы контролируемой зоны, а также на внешние провода и кабели, проходящие через помещения с основным и вспомогательным оборудованием, а также на металлические трубы и другие проводящие конструкции.

Для оценки защищенности помещений от утечки звуковой информации следует учитывать возможность прослушивания как из соседних помещений, так и с улицы. Также стоит провести оценку возможности разведки с использованием лазерных микрофонов и учесть каналы утечки через вибрации, вызванные акустическими волнами в твердых материалах.

Эффективность защиты информации определяется ее своевременностью, активностью, непрерывностью и комплексностью. Очень важно проводить защитные мероприятия комплексно, то есть обеспечивать нейтрализацию всех опасных каналов утечки информации. Необходимо помнить, что даже один-единственный не закрытый канал утечки может свести на нет эффективность системы защиты.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации – неконтролируемый выход конфиденциальных сведений за пределы предприятия, помещения, здания, какой-либо территории или круга лиц, которым доверили хранение информации ограниченного круга лиц. Утечка происходит по каналам передачи данных. Неконтролируемые каналы нарушают безопасность систем защиты.

Специалисты выделяют три группы способов утечки информации:

- технические каналы утечки информации;
- визуальные и визуально-оптические;
- материально-вещественные.

В данной работе будет рассматриваться только технические каналы утечки информации.

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

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

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.

Далее полученная информация преобразуется 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. Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал (усиление) и преобразует информацию в форму сигнала, доступную получателю (человеку или техническому устройству).

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.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Приемник выполняет функцию, обратную функции передатчика. Он производит:

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

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:

- дальний инфракрасный поддиапазон 100 - 10 мкм (3 - 300 ТГц);

- средний и ближний инфракрасный поддиапазон 10 - 0,76 мкм (30 - 400 ТГц);
- видимый диапазон (сине-зелёно-красный) 0,76 - 0,4 мкм (400 - 750 ТГц).

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. Он подразделяется на:

- низкочастотный 10 - 1 км (30 - 300 кГц);
- среднечастотный 1 км - 100 м (300 кГц - 3МГц);
- высокочастотный 100 - 10 м (3 - 30 МГц);
- ультравысокочастотный 10 - 1м (30 - 300 МГц);
- и т.д. до сверхвысокочастотного 3 - 30 ГГц (10 - 1 см).

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Здесь различают:

- инфразвуковой диапазон 1500 - 75 м (1 - 20 Гц);
- нижний звуковой 150 - 5 м (1- 300 Гц);
- звуковой 5 - 0,2 м (300 - 16000 Гц);
- ультразвуковой < 0,2 м (> 16000 Гц) и до 4 МГц

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Нормативные документы по противодействию технической разведке:

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

2.2 Указы Президента Российской Федерации

- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- «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;
- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212;
- «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;

2.3 Постановления Правительства Российской Федерации

- 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 Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233.
- «О сертификации средств защиты информации» от 26 июня 1995 г. №608.
- «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.
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973.
- «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.

2.4 Решения Гостехкомиссии России

- «Основы концепции защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам» от 16 ноября 1993 г. № 6.
- «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации» от 14 марта 1995 г. № 32.
- «Типовое положение о Совете (технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам» от 14 марта 1995 г. № 32.
- «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (учреждении, организации)» от 14 марта 1995 г. № 32.

- «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте» от 3 октября 1995 г. № 42.
- «Методические рекомендации по разработке развернутых перечней сведений, подлежащих засекречиванию» от 3 февраля 1995 г. № 29.
- «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)» от 23 мая 1997 г. № 55.
- «Положение о государственном лицензировании деятельности в области защиты информации (Решение Гостехкомиссии России и ФАПСИ)» от 27 апреля 1994 г. № 10 с дополнениями и изменениями, внесенными Решением Гостехкомиссии России и ФАПСИ от 24 июня 1997 г. № 60.
- Положение о головной научно-исследовательской организации по проблеме защиты информации (Решение Председателя Гостехкомиссии России) от 15 марта 1993 г.
- Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР (Пособие к ВСН-01-82). Утверждено НИИА и согласовано с Гостехкомиссией СССР в 1983 г., переутверждено Решением Гостехкомиссии России от 13 ноября 1990 г, № 89–3.
- «О защите информации при вхождении России в международную информационную систему «Интернет» от 21 октября 1997 г. № 61.

2.5 Руководящие и нормативно-методические документы Гостехкомиссии

- Руководящий документ (РД). Защита от несанкционированного доступа (НСД) к информации. Термины и определения. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.
- РД Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.
- РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по ЗИ. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

– РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

– РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

– РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 25 июля 1997 г.

– РД. Защита информации Специальные защитные знаки. Классификация и общие требования. Решение Председателя Гостехкомиссии России от 25 июля 1997г.

– Нормативно-методические документы (НМД) по противодействию (ПД) средствам иностранной радиотехнической разведки. Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

– Нормативно-методические документы по противодействию иностранной радиоразведке. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

– Нормативно-методические документы по противодействию средствам иностранной фоторазведки и оптикоэлектронной разведки. Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

– Нормативно-методические документы по противодействию средствам иностранной гидроакустической разведки. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

– Нормативно-методические документы по противодействию радиолокационным средствам иностранной воздушной и космической разведок. Решение Гостехкомиссии России от 16 ноября 1993г. № 7.

– Нормативно-методические документы по противодействию радиационной разведке. Решение Гостехкомиссии России от 15 ноября 1994 г. № 25.

– Нормативно-методические документы по противодействию тепловизионным средствам иностранной инфракрасной разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

- Нормативно-методические документы по противодействию средствам иностранной химической разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.
- Нормативно-методические документы по противодействию средствам иностранной разведки лазерных излучений. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.
- Нормативно-методические документы по противодействию средствам иностранной акустической (речевой) разведки. Решение Гостехкомиссии России. 1991 г.
- Нормы эффективности защиты АСУ и ЭВТ от утечки информации за счет ПЭМИН. Решение Председателя Гостехкомиссии СССР, 1977 г.
- Нормы эффективности защиты технических средств передачи телевизионной информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13, от 30 ноября 1987г. № 11-3.
- Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13.

3 СТРУКТУРНАЯ МОДЕЛЬ И АНАЛИЗ ЗАЩИЩАЕМОГО ОБЪЕКТА

3.1 Структура организации

Наименование организации: ООО “Динамика”.

Область деятельности: IT консалтинг и разработка ПО.

Организационная структура предприятия состоит из следующих подразделений:

- руководство предприятия (директор);
- специалист по ИБ;
- отдел бухгалтерии;
- отдел анализа данных;
- отдел разработки ПО;
- отдел продаж;
- отдел кадров.

Схематическое представление изображено на рисунке 2.

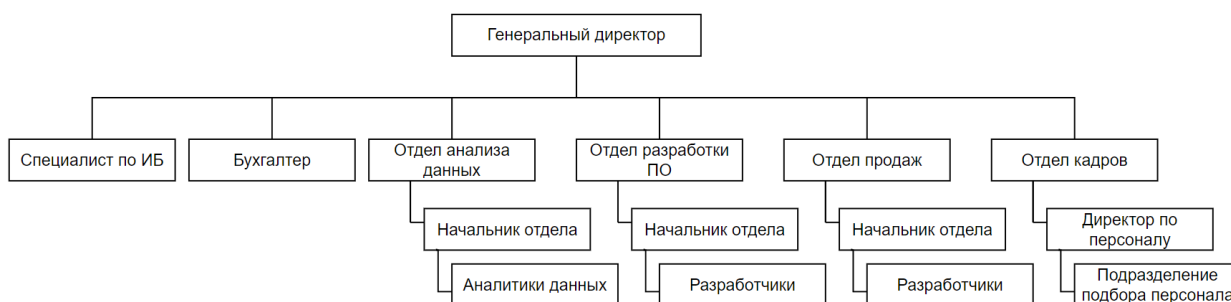


Рисунок 2 – Организационная структура предприятия

Защищаемая информация:

- коммерческая тайна - сведения о заключенных договорах и контрактах, данные о партнерах и клиентах компании, информация о ценовой политике и финансовых операциях;
- техническая информация конфиденциального характера - состав и структура баз данных, содержащих информацию клиентов маркетплейсов, конфигурации используемого серверного и сетевого оборудования, сведения об архитектуре и настройках корпоративных информационных систем;
- государственная тайна - проекты для государственных учреждений или оборонных организаций, информация о разработке систем защиты от киберугроз, криптографии или технологий, обеспечивающих конфиденциальность данных

В рамках выбранного объекта защиты действует структура, приведенная на рисунке 3. Красными стрелками обозначены закрытые потоки информации, зелеными стрелками – открытые потоки информации.

В закрытых потоках циркулирует информация о внутренней и внешней деятельности, а также информация из внутренней информационной системы.

К открытым потокам относится информация о найме сотрудников, информация, передаваемая СМИ, для взаимодействия с общественностью, а также информация о материально техническом снабжении

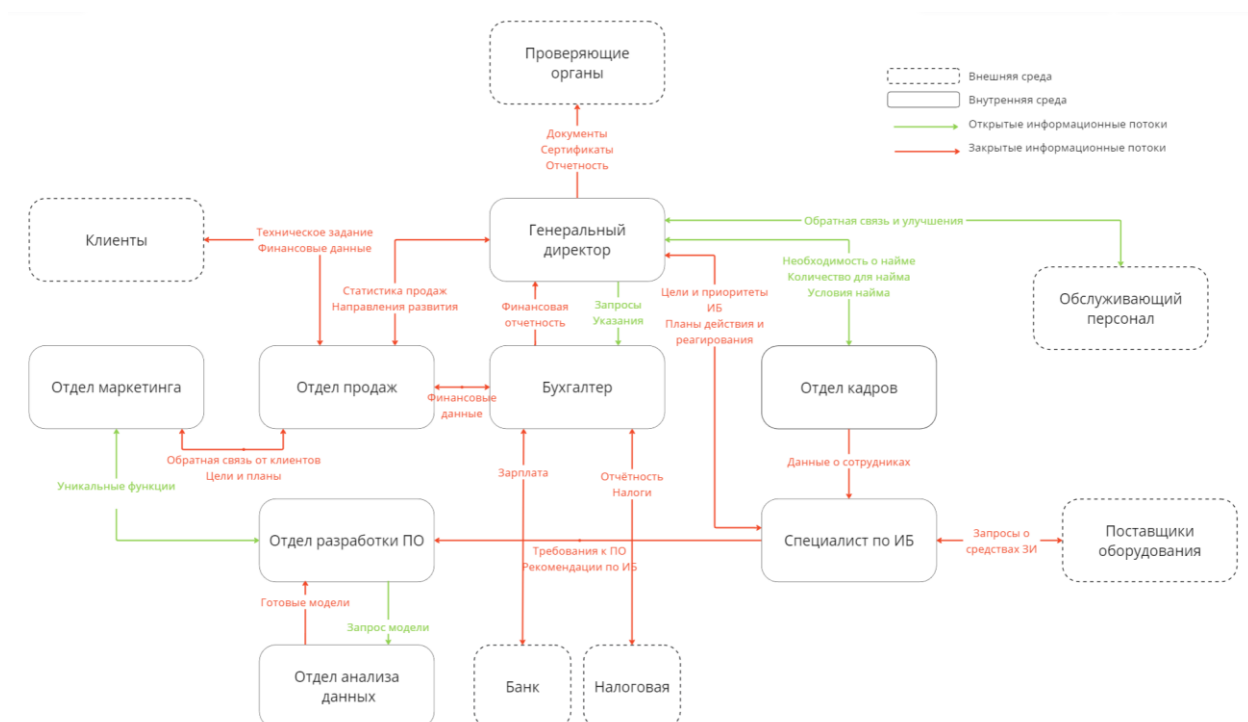


Рисунок 3 – Информационные потоки организации

Государственная тайна (уровень секретно) – проектные работы, технологии, данные, имеющие важное экономическое значение, влияющее на безопасность государства. Система имеет 3 тип формы доступа для граждан, допускаемых к секретным сведениям.

3.2 Обоснование защиты информации

Так как одной из составляющих информации организации "Динамика" является информация, составляющая государственную тайну, то опираться следует на закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Постановление Правительства РФ от 15.04.1995 N 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." и Постановление Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51 "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам".

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.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 1, пункту 4, защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 3, пункту 26, защита информации осуществляется путем:

2) предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

5) выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

6) предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

3.3 Описание инженерно-технических показателей объекта

Рассмотренный в данной курсовом проекте объект защиты представляет собой помещение, расположенное на 7 этаже бизнес-центра. План помещения представлен на рисунке 4. Помещения на плане пронумерованы в соответствии с названиями:

1. Кабинет директора

2. Ресепшн
3. Переговорная
4. IT отдел
5. Кабинет бухгалтерии
6. Серверная
7. Обеденная зона
8. Коридор
9. Щитовая

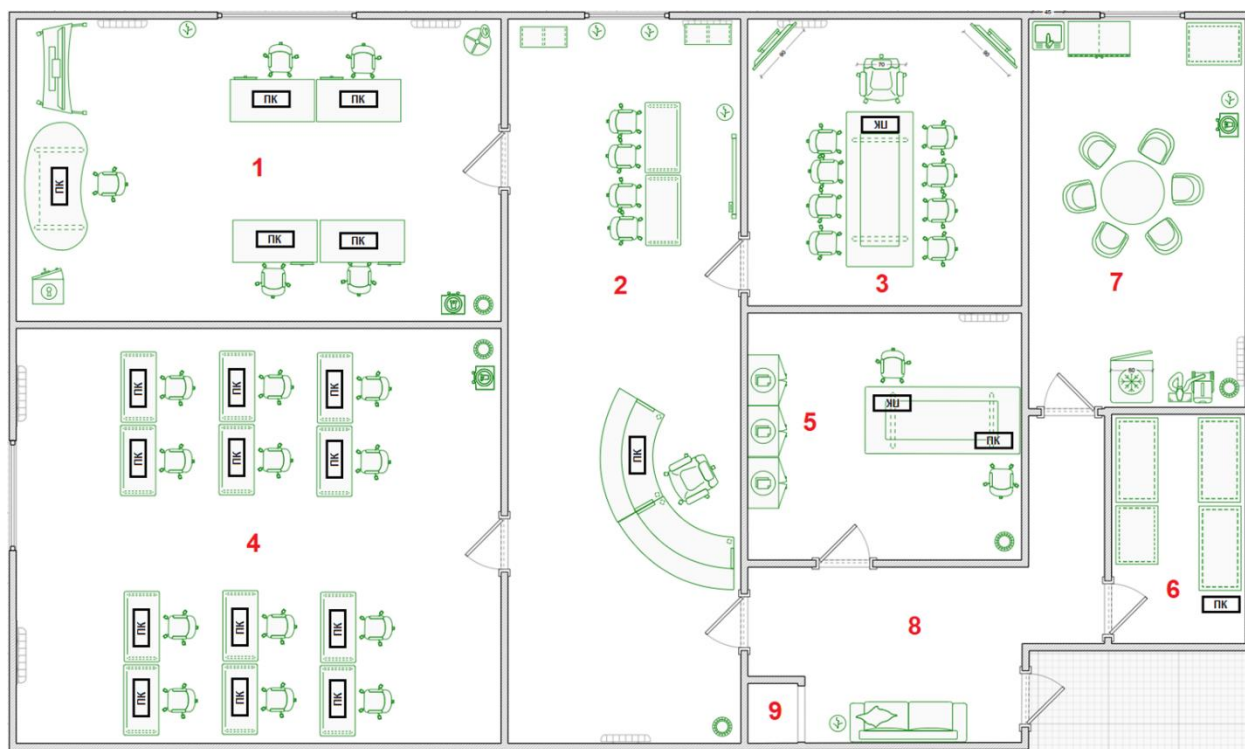














Рисунок 4 – План защищаемого помещения

Таблица 1 – Условные обозначения

Обозначение	Описание
	Рабочий стол
	Рабочий стол с ящиком
	Стул

	Вешалка
	Горшок с цветами
	Сейф
	Куллер
	Мусорка
	Шкаф с документами
	Раковина
	Пылесос
	Батарея
	Персональный компьютер
	Телевизор
	Диван

Помещения, требующие защиты:

1. Переговорная: 3.9м х 4.08м, 15.91м²
2. Кабинет директора: 6.9м х 4.3м, 29.67м²
3. IT отдел: 6.9м х 5.9м, 40.71м²
4. Серверная: 1.9м х 3.2м, 6.21м²

Для ведения переговоров предназначено два помещения (кабинет директора и переговорная). В переговорной находятся: стол, 8 стульев, 2 экрана, компьютер, 2 розетки, 1 батарея центрального отопления.

В кабинете директора: 1 окно, 5 столов, 5 стульев, 5 компьютеров, 4 розетки, 2 батареи центрального отопления, растение, сейф, кулер, вешалка для одежды.

В IT отделе 2 окна, 2 батареи центрального отопления, 12 рабочих мест с ПЭВМ, 12 розеток, кулер.

В серверной располагается 4 серверные стойки, 1 ПЭВМ, 4 розетки.

Помещение расположено на 7 этаже бизнес-центра, 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. В помещениях присутствуют декоративные элементы (растения, кулер), где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны каналы электрического и электромагнитного утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому. Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение активными и пассивными средствами защиты информации.

Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

В таблице 2 представлены активные и пассивные средства защиты.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустический, акустоэлектрический	проводка, двери, окна	усиленная звукоизоляция, в том числе вентиляции, доводчики на двери,	устройства акустического защумления

		утолщение дверей, фильтры для сетей электропитания	
вибрационный виброакустический	батареи, трубы, стены, пол, окна, двери	обшивка стен, дополнительное тамбурное помещение, дополнительные поглощающие накладки на радиаторы и трубы тепло- и водоснабжения	устройства вибрационного зашумления
оптический	окна, двери	жалюзи на окна, затемненное остекление, доводчики на двери, правильная планировка (экраны ПЭВМ не расположены в прямой видимости)	блокирующие обзор устройства
электромагнитный электрический	ПЭВМ, бытовые приборы, телевизоры, розетки	фильтр для сетей электропитания, экранирование помещения, осуществление развязки по цепям питания	устройства электромагнитного зашумления

4 АНАЛИЗ И СРАВНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Устройства противодействия утечке информации по акустическому и виброакустическому каналам

Пассивная защита представляет собой:

- усиленные двери;
- изолирующие звук и вибрацию материалы стен.

В качестве пассивной защиты выбраны звукоизоляционный усиленные двери Rw Prima M900 стоимостью 34 050 руб.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Ниже в таблице 3 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналам.

Таблица 3 – Сравнительный анализ средств активной защиты для виброакустического канала

	ЛГШ-402	ЛГШ-403	Шорох-5Л	СОНАТА АВ-4Б
Сертификация и соответствие требованиям	Соответствует требованиям по 4-му классу защиты	Соответствует требованиям по 3-му классу защиты	Соответствует требованиям по 1-му классу защиты	Соответствует требованиям по 1-му классу защиты
Генератор шума	Есть. Размеры 145 x 100 x 50 мм.	Есть. Размеры 82 x 67 x 22 мм.	Отсутствуют	Есть
Вибропреобразователи	Габаритные размеры не более 40 x 25 мм	Габаритные размеры не более 40 x 25 мм	«ПЭД-8А» Габаритные размеры не более 35 x 30 мм	«Соната-СВ-4Б1» Габаритные размеры не более 19 x 47 мм
Акустические излучатели	Габаритные размеры не более 66 x 66 x 25 мм	Габаритные размеры не более 66 x 66 x 25 мм	«АИ-8А/Н» и «АИ-8А/Мини» Габаритные размеры не более 170 x 71 мм	«Соната-СА4Б» и «Соната-СА4Б1» Габаритные размеры не более 53 x 38 мм

Напряжение питания	187 / 242 В	176 / 230 В	220 В +-15%	220 В
Диапазон рабочих частот	175 / 11 200 Гц	170 / 12 900 Гц	190 / 11 700 Гц	175 / 11200
Потребляемая мощность	Не более 20 ВА	Не более 2,5 В	Не более 130 ВА	Не менее 10 В
Интервал уровня регулировки звукового давления	Не менее 35 дБ	не менее 40 дБ	Не менее 30 дБ	Не менее 35 дБ

По результатам анализа была выбрана система ЛГШ-403, стоимость которой равна 6 000 рублей, не включая комплектующие. Выбрана она по соотношению характеристик рабочих частот, интервалу звукового давления и размерами.

В состав ЛГШ-403 входят:

- Генератор шума ЛГШ-403
- Вибропреобразователь для стен, полов, потолков ЛВП-2с
- Вибропреобразователь для окон ЛВП-2о
- Акустический излучатель ЛВП-2а
- Вибропреобразователь для трубопроводов ЛВП-2т
- Размыкатели ЛУР

4.2 Устройства противодействия утечке информации по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи или шторы. С точки зрения удобства содержания были выбраны Blackout-жалюзи стоимостью 4600 рублей в кабинете директора и IT отдел.

4.3 Устройства противодействия утечке по электромагнитным и электрическим каналам

Пассивная защита основывается на установке фильтров для сетей электропитания во

всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. Устройства активной защиты представлены в Таблице 4.

Таблица 4 – Сравнительный анализ средств активной защиты

Изделие	ЛГШ - 503	ЛГШ-513	Соната-РС2
Соответствует требованиям документов	Соответствует требованиям по 2-му классу защиты	Соответствует требованиям по 2-му классу защиты	Соответствует требованиям по 1-му классу защиты
Диапазон частот	0,01–1800 МГц	0,009–1800 МГц	0.01–2000 МГц
Диапазон регулировки уровня шума	Не менее 20 дБ	Не более 20 дБ	Не менее 35 дБ
Потребляемая мощность	Не более 45 ВА	Не более 45 ВА	Не более 10 Вт
Цена	44 200 руб.	39 000 руб.	24 000 руб.

После проведения анализа было решено использовать ЛГШ-513 стоимостью 39 000 рублей в качестве средства защиты. Его выбор обусловлен широким спектром защиты, охватывающим электрические, электромагнитные каналы и предотвращающим ПЭМИН. При этом стоимость данного средства приемлема, особенно при условии закрытия нескольких потенциальных точек утечки.

В результате анализа рынка сетевых фильтров была выявлена модель, являющаяся наиболее популярной среди покупателей в разных магазинах: сетевой фильтр Power Cube SPG-B-10. Данная модель отличается надежностью и небольшой ценой в 1000 рублей.

5 РАССТАНОВКА ВЫБРАННЫХ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СЗИ НА ПЛАНЕ

Выбранные нами средства защиты:

- система постановки виброакустических и акустических помех ЛГШ-403;
- генератор шума ЛГШ-513;
- сетевой фильтр Power Cube SPG-B-10
- жалюзи
- усиленные двери RwPrima M900.

Общая смета представлена в таблице 5.

Для ЛГШ-403 предусмотрены рекомендуемые правила установки:

- для стен: один вибропреобразователь ЛВП-2с на каждые 6 м²;
- для полов и потолков: один вибропреобразователь ЛВП-2с на каждые 6 м²;
- для окон: один вибропреобразователь ЛВП-2о на каждое стекло или ЛВПv2т на раму каждого оконного проема, или один акустический излучатель ЛВП-2а на межрамное пространство (в случае использования оконных блоков с 2-мя или 3-мя раздельными рамами);
- для трубопроводов: один вибропреобразователь ЛВП-2т на каждый независимый участок инженерно-технических коммуникаций (например, водопровод и т.д.);
- для воздуховодов, вентиляции, двойных дверных коробок и прочих замкнутых объемов: по одному акустическому излучателю ЛВП-2а на каждые 40 м² каждого замкнутого объема.

На рисунке 5 представлена итоговая схема расстановки инженерно-технических средств защиты информации.

Таблица 5 – Общая смета

Устройство	Цена за единицу, руб	Количество, шт.	Стоимость, руб
Вибропреобразователь для стен, полов, потолков ЛВП-2с	3640	20	72 800
Вибропреобразователь для окон ЛВП-2о	3640	2	7280

Вибропреобразователь для труб ЛВП-2т	3640	5	18 200
Акустический извещатель ЛВП-2а	5200	3	15 600
ЛГШ-513	39000	4	156 000
Размыкатели ЛУР	5590	5	27 950
Генератор зашумления ЛГШ-403	19400	2	38 800
Усиленная дверь Rw Prima M900	34050	4	136 200
Blackout-жалюзи 2х3м	5280	2	10 560
Итого			483 390

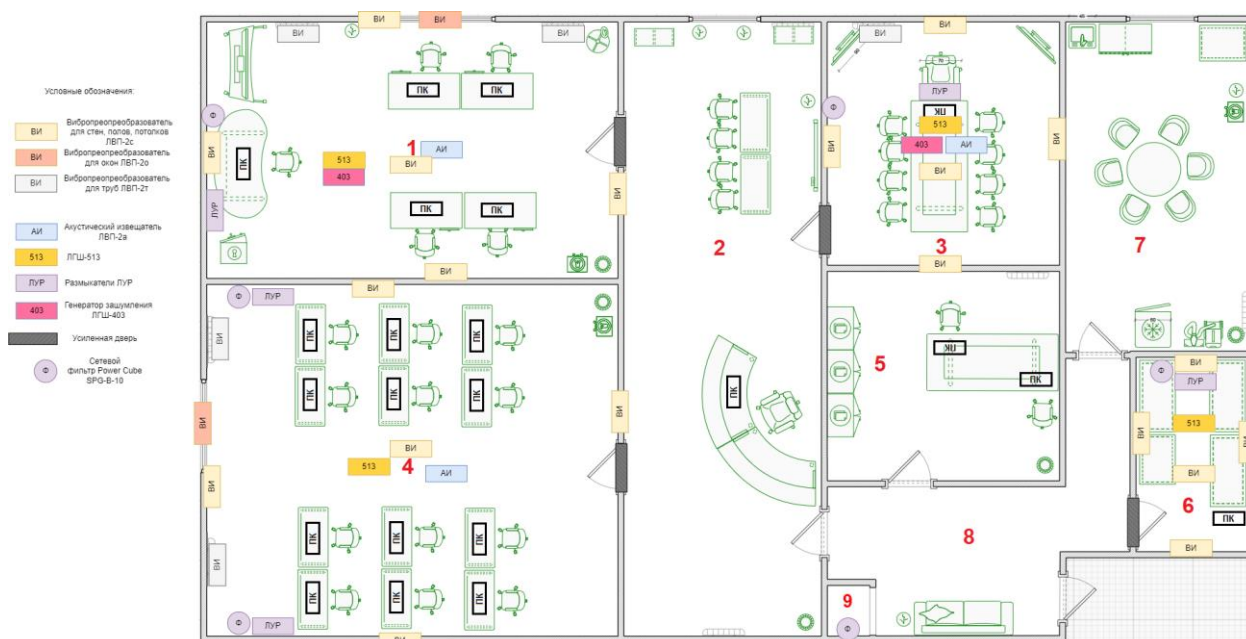


Рисунок 5 – Схема расстановки СЗИ

ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта, мной была разработана инженерно-техническая система защиты информации для организации ООО “Динамика”.

Для достижения цели мною было проведено предпроектное обследование организации и выявлены основные информационные активы, внешние и внутренние, открытые и закрытые информационные потоки, а также был обследован план помещения организации и выявлены возможные каналы утечки информации.

Также мною был проведен анализ нормативной базы, с целью выявления обоснования для защиты информации и анализ рынка инженерно-технических средств, с целью выявления наилучших предложений.

Результатом обследования организации и анализа нормативной базы является план помещения предприятия с инженерно-технической системой защиты информации.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

5. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
6. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
7. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
8. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 14.09.2023)