

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Проектирование инженерно-технической системы защиты информации на предприятии»

Выполнил:

Чан Ван Хоанг, студент группы N34511



(подпись)

Проверил:

К.т.н., доцент фБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Чан Ван Хоанг (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Технологии защиты информации (2020)
Руководитель	Попов Илья Юрьевич к.т.н., доцент факультета безопасности информационных технологий (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

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

Содержание пояснительной записки

Пояснительная записка включает разделы: введение, анализ технических каналов утечки информации, руководящие документы, анализ защищаемых помещений, анализ рынка технических средств, расстановка технических средств, заключение, список использованных источников.

Рекомендуемая литература

1. 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

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	Чан Ван Хоанг (Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Чан Ван Хоанг
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34511

Направление (специальность) 10.03.01 Технологии защиты информации (2020)

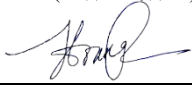
Руководитель Попов Илья Юрьевич
к.т.н, доцент факультета безопасности информационных технологий
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	15.11.2023	15.11.2023	
2	Анализ теоретической составляющей	01.12.2023	01.12.2023	
3	Разработка комплекса инженернотехнической защиты информации в заданном помещении	10.12.2023	10.12.2023	
4	Представление выполненной Курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Чан Ван Хоанг 
(Подпись, дата)

Студент	Чан Ван Хоанг (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Технологии защиты информации (2020)
Руководитель	Попов Илья Юрьевич к.т.н, доцент факультета безопасности информационных технологий (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

1. Цель и задачи работы

☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Целью работы является повышение защищенности рассматриваемого помещения. Задачами являются анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

2. Характер работы ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое: Исследование

Курсовая работа соержит Введение; Анализ технических каналов утечки информации; Перечень руководящих документов; Анализ защищаемого помещения; Анализ рынка технических средств; Расстановка технических средств; Заключение; Список использованных источников
--

В результате работы была предложена защита от утечек информации по акустическому, оптико-виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, электронному техническим каналам защиты информации, обеспечена защита от ПЭМИН.

4

СОДЕРЖАНИЕ

Содержание	5
Список сокращений.....	6
Введение	7
1 Анализ технических каналов утечки информации.....	8
1.1 Акустический канал утечки.....	9
1.2 Материально-вещественный канал утечки	10
1.3 Визуально-оптический канал утечки.....	10
1.4 Электромагнитный канал утечки	10
2 Перечень руководящих документов	12
3 Анализ защищаемых помещений.....	14
3.1 План помещений и информационные потоки предприятия.....	14
3.2 Описание помещений.....	16
3.3 Анализ возможных утечек информации	16
3.4 Выбор средств защиты информации	16
4 Анализ технических средств защиты информации.....	18
4.1 Требования к защите помещений	18
4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации	18
4.3 Анализ СЗИ для электромагнитного, электрического каналов	20
4.4 Анализ СЗИ для визуально-оптического канала	21
5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ	22
Заключение.....	26
Список использованных источников.....	27

СПИСОК СОКРАЩЕНИЙ

ЛВС – Локальная вычислительная сет

ЭВМ - Электронная вычислительная машина

ПО – Программное обеспечение

ОС - Операционная система

ARP - Address Resolution Protocol

DHCP - Dynamic Host Configuration Protocol

MAC – Media Access Control

ВВЕДЕНИЕ

Любое современное предприятие функционирует на основе обработки и управления информацией. Обеспечение безопасности информации становится важным аспектом, поскольку широко используемые технологии без должной осторожности могут стать источником проблем.

Средства защиты информации (СЗИ) направлены на обеспечение безопасности информации в информационных системах. Эти системы представляют собой набор данных, которые хранятся в базах данных, использующих информационные технологии для обработки данных, а также технические средства. СЗИ помогают предотвратить несанкционированный доступ к ресурсам и данным предприятия, снижая риск утечки, уничтожения, искажения, копирования и блокирования информации. Такие меры также минимизируют экономический, репутационный и другие виды ущерба, который может быть причинен предприятию. Разработка эффективных методов для решения этой задачи становится одной из самых важных проблем нашего времени. Технические средства защиты информации представляют собой важную часть системы обеспечения конфиденциальности на предприятии.

В данной работе исследуется процесс разработки комплексной инженерно-технической защиты информации, содержащей государственную тайну с уровнем "совершенно секретно" на предприятии. Объект защиты включает кабинет директора, переговорную, офисы и серверные помещения.

Работа состоит из пяти глав. Первая глава анализирует технические каналы утечки информации. Вторая глава содержит перечень управляющих документов, а третья глава проводит анализ помещений, подлежащих защите, с точки зрения возможных утечек информации и необходимости защиты техническими средствами. Четвертая глава представляет собой анализ рынка технических средств защиты информации различных категорий, а пятая глава посвящена разработке схемы размещения выбранных технических средств в защищаемых помещениях. В данной курсовой работе будут рассмотрены локальная вычислительная сеть, атаки и методы защиты в ЛВС.

Цель работы - повышение защищенности рассматриваемого помещения.

Для достижения цели необходимо решить следующие задачи:

- проанализировать защищаемое помещение;
- оценить каналы утечки информации;
- выбрать меры пассивной и активной защиты информации.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Под техническим каналом утечки информации понимают совокупность источника конфиденциальной информации, среды распространения и средства технической разведки. На рисунке 1 показана структурная схема ТКУИ.

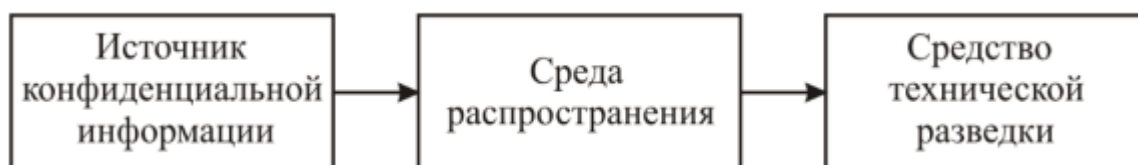


Рисунок 1 – Технический канал утечки информации

При обнаружении потенциальных каналов утечки информации важно учитывать все компоненты системы, включая основное оборудование технических средств обработки информации (ТСОИ), конечные устройства, соединительные линии, устройства для распределения и коммутации, системы электропитания, заземления и другие элементы.

Кроме основного оборудования, непосредственно связанного с обработкой и передачей информации, также следует учитывать вспомогательные технические средства и системы (ВТСС). Эти элементы также могут представлять потенциальные уязвимости и способы, через которые информация может быть скомпрометирована или утекла.

Каналы утечки информации по физическим принципам можно разделить на следующие группы:

- акустический;
- материально-вещественный;
- визуально-оптический;
- электромагнитный.



Рисунок 2 – Каналы утечки информации

1.1 Акустический канал утечки

Наиболее ценной акустической информацией чаще всего является речь, однако необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

Акустический канал утечки информации реализуется в следующем:

- подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны;
- негласная запись разговоров на диктофон или магнитофон (в том числе цифровые диктофоны, активизирующиеся голосом);
- подслушивание разговоров с использованием выносных микрофонов.

Для предотвращения утечки информации по акустическому каналу необходимо использовать звукоизолирующие материалы, препятствующие распространению акустического сигнала за пределами помещения.

1.2 Материально-вещественный канал утечки

Особенность материально-вещественного канала утечки информации состоит в том, что его наличие позволяет получать секретные сведения, находясь за пределами предприятия. Для получения информации изучаются внешние признаки объектов, физические и химические свойства твердых, газообразных и жидких веществ, случайно попадающих в окружающую среду с территории производства.

В структуру канала, по которому происходит утечка информации, входят:

- источники данных;
- линии физического перемещения носителей информации по каналу (людей или вещественных объектов);
- технические средства перехвата информационных сигналов.
- о деятельности предприятия судят по так называемым «демаскирующим признакам», которые обнаруживаются с помощью специальных средств и приборов.
- демаскирующие признаки подразделяют на следующие группы:
- видовые (цвет, структура поверхности, форма предметов);
- сигнальные (параметры излучений: мощность, амплитуда, диапазон);
- вещественные (ими являются физические и химические характеристики объектов).

Для получения конфиденциальных данных по таким каналам утечки информации злоумышленники используют прямые и косвенные демаскирующие признаки объектов.

1.3 Визуально-оптический канал утечки

Если экран монитора или часть лежащих на столе документов можно увидеть через окно офиса, возникает риск утечки. Для борьбы с этим способом необходимо применять в большинстве случаев простые технические средства:

- снижение отражательных характеристик и уменьшение освещенности объектов;
- использование светоотражающих стекол, различных преград и маскировок;
- расположение объектов так, чтобы свет от них не попадал в зону возможного перехвата.

1.4 Электромагнитный канал утечки

Электромагнитный канал утечки информации – физический путь от источника побочных электромагнитных излучений и наводок различных технических средств к

злоумышленнику за счёт распространения электромагнитных волн в воздушном пространстве и направляющих системах.

Представляет опасность также перехват информации, содержащейся в побочных электромагнитных излучениях. Электромагнитные волны, распространяясь в пределах электромагнитного поля на небольшом расстоянии, также могут быть перехвачены. Они могут исходить:

- от микрофонов телефонов и переговорных устройств;
- от основных цепей заземления и питания;
- от аналоговой телефонной линии;
- от волоконно-оптических каналов связи;
- из других источников.

Перехватить и расшифровать их не представляет сложности для современных технических средств.

Технологии позволяют подключать закладные устройства ПЭМИН (термин расшифровывается как «побочные электромагнитные излучения и наводки») непосредственно к цепям питания или же установить в мониторе или корпусе компьютера, при этом они через внутренние подсоединения к платам могут перехватывать данные:

- выводимые на экран монитора;
- вводимые с клавиатуры;
- выводимые через провода на периферийные устройства (принтер);
- записываемые на жесткий диск и иные устройства.

Способами борьбы в этом случае станут заземление проводов, экранирование наиболее явных источников электромагнитного излучения, выявление закладок или же использование специальных программных и аппаратных средств, позволяющих выявить закладки. Но информация, передаваемая по сети Интернет, является доступной для перехвата. Здесь борьба с ее хищениями может осуществляться и аппаратными, и программными техническими средствами.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;
- Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Межведомственная комиссия по защите государственной тайны решение No 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

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.
- 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.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 План помещений и информационные потоки предприятия

Перед началом проектирования инженерно-технической защиты помещений необходимо изучить все открытые и закрытые информационные потоки, которые фигурируют на предприятии ООО «TVH».

Область деятельности: Информационная технология (разработка программного обеспечения, информационную безопасность, управление проектами, ИТ-инфраструктуру и другие области).

Закрытые информационные потоки: к

- конфиденциальные данные клиентов и пользователей;
- разработка программного обеспечения и кодовые базы;
- информация об уязвимостях и стратегиях безопасности.

Открытые информационные потоки:

- общедоступная информация о продуктах или услугах компании;
- публичные образцы программного обеспечения или решений;
- информация о предприятии и его структуре.

Перечень защищаемых информационных активов:

- данные клиентов и пользователей;
- интеллектуальная собственность;
- коммерческая информация;
- данные организации;
- информационная инфраструктура;
- физические ресурсы;
- партнерские и контрактные данные.

На рисунке 3 представлены информационные потоки предприятия.

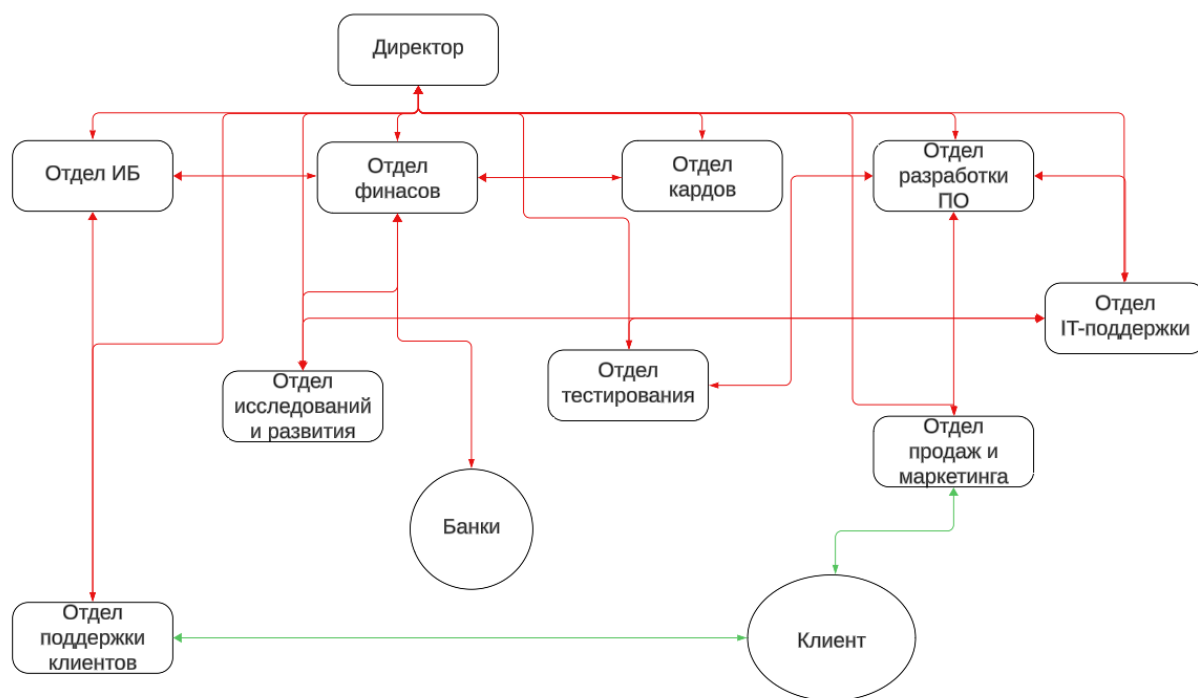


Рисунок 3 – Открытые и закрытые информационные потоки предприятия

Также на рисунке 4 представлен план защищаемого помещения с учетом мебелировки.

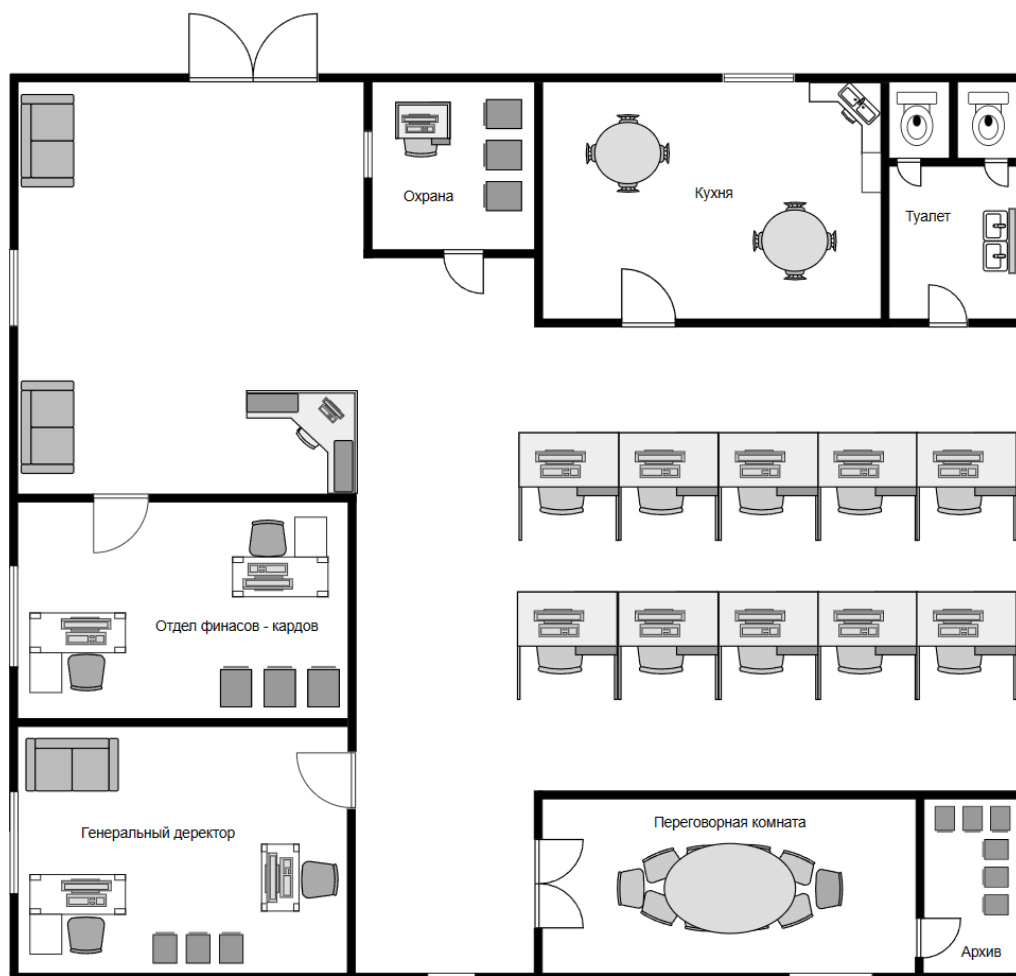


Рисунок 4 – План помещения

3.2 Описание помещений

В соответствии с степенью защищенности информации защите подлежат следующие помещения, приведенными в таблице 1.

Таблица 1 – Описание помещений

Название комнаты	Площадь (м ²)	Устройство
Кабинет директора	20	2 ПК, 2 стола, 2 стула, 1 диван, 3 шкафа
Переговорная комната	24	1 стол, 10 стульев
Архив	8	6 шкафов
Отдел финансов – кадров	20	2 ПК, 2 стула, 2 стола, 3 шкафа
Кухня	20	2 стола, 8 стульев
Охрана	12	1 ПК, 3 шкафа
Рабочая зона сотрудника	36	10 ПК, 10 стульев, 10 столов
Зон отдыха	30	1 ПК, 1 стол, 1 стул, 2 дивана

3.3 Анализ возможных утечек информации

В помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому.

3.4 Выбор средств защиты информации

Для реализации инженерно-технической защиты, соответствующей 2 уровню секретной информации «совершенно секретно», необходимо оборудовать помещение СЗИ, приведенными в таблице 2.

Таблица 2 – Средства защиты информации

Каналы	Источники	Пассивная защита	Активная защита
Акустический	Окна, двери, электрические сети,	Звукоизоляция переговорной,	Устройства акустического

	проводка	фильтрация сетей электропитания	зашумления
Визуально- оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, ПК, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного зашумления
Вибрационный, виброакустический	Все твердые поверхности помещения	Дополнительное помещение перед переговорной, изолирующие звук и вибрацию обшивки стен	Устройства вибрационного зашумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Требования к защите помещений

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:

- стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см.
- в помещениях для работы с гостайной 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 см. Дверь устанавливается на металлический каркас.
- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
- по требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
- все режимные помещения оборудуются аварийным освещением.

4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита: усиленные двери, дополнительная отделка переговорной звукоизолирующими материалами, тамбурное помещение перед переговорной. В качестве пассивных средств были выбраны: шумоизоляция стен, звукоизолирующие двери.

Активная защита: система виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «совершенно секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б.

Ниже в таблице 3 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналам.

Таблица 3 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Описание	Цена, руб
SEL SP-55-2A	Диапазон частот: 100-5600 гц	Генератор виброакустических помех с эквалайзером, осуществляющий активную защиту от утечки информации по акустическому и виброакустическому каналу. Система гарантированно защищает от стетоскопных/контактных микрофонов, микроволновых систем (в т.ч. лазерных микрофонов) и других устройств, использующих для дистанционного съема речевой информации оконные проёмы и их остекление, стены, потолки, полы, трубопроводы газо- и водоснабжения, вентиляционные шахты и т.д. Система собрана по модульному принципу.	14,000
Генератор маскирующего шума «Камертон- 5»	Диапазон рабочих частот 90 - 11200 Гц	Комплекс технических средств для защиты речевой информации от несанкционированного съема через виброакустические каналы. Гарантирует невозможность прослушки разговоров посредством лазерных и направленных микрофонов через окна, инженерные коммуникации, вентиляцию, межкомнатные перегородки, пр.	46,000
«Соната АВ-4Б»	Диапазон частот: 175 – 11200 Гц	Блок электропитания и управления, генератор- акустоизлучатель, генераторвибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт	44,200

		управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптикоэлектронному (лазерному) каналу, генераторный блок "АВ- 4Л", вибровозбудитель "СП-4Л".	
--	--	---	--

По результатам анализа была выбрана система «Соната АВ-4Б» . “Соната-АВ” 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)". Данная система имеет сертификат ФСТЭК, достаточную комплектацию и приемлемую стоимость. Благодаря этому построению проявляется высокая стойкость защиты информации. Уменьшить затраты благодаря использованию единой линии связи и электропитания. Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы.

4.3 Анализ СЗИ для электромагнитного, электрического каналов

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.

Ниже в таблице 4 приведен сравнительный анализ подходящих средства активной защиты помещений по электромагнитному, электрическому каналов.

Таблица 4 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Описание	Цена, руб
Соната РС2	Частотный диапазон до 2ГГц, регулировка уровня шума в 3 частотных полосах.	SEL SP-44 Сертификат ФСТЭК 1445, Класс устойчивости к импульсным помехам 5/50 нс (ГОСТ Р 51317.4.4-99), Генератор регулируемого шума. Индикация	23,600

		нормального/аварийного режима работы	
SEL SP-44	Диапазон частот: 0,01-300 МГц	SEL SP-44 Сертификат ФСТЭК 1445, Класс устойчивости к импульсным помехам 5/50 нс (ГОСТ Р 51317.4.4-99), Генератор регулируемого шума. Индикация нормального/аварийного режима работы	24,000

В результате анализа был выбран генератор шума «Анна» Соната РС2. Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

Дополнительно был выбран «Соната-РЗ» средство активной защиты информации от утечки за счет ПЭМИН, так как оно обладает лучшими характеристиками по сравнению с другими средствами пассивной защиты от ПЭМИН.

4.4 Анализ СЗИ для визуально-оптического канала

Применять средства ослабления отраженного света — шторы, жалюзи, темные или матовые стекла, иные ограждения, затрудняющие распространение сигнала.

Были выбраны рулонные шторы Роллайт 2 с технологией BlackOut 100 см * 150 см 3190 руб/шт.

5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

На основании таблиц 3 и 4 были выбраны следующие средства защиты информации:






- система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б;








- генератор шума «Анна» Соната РС2.

- «Соната-РЗ» средство активной защиты информации от утечки за счет ПЭМИН

- рулонные шторы Роллайт 2 с технологией BlackOut 100 см * 150 см
- усиленные звукоизоляционные двери Phoenix (звукоизоляционная прокладка с металлической сеткой: толщина 10 мм, обшивка: металл 3 мм, устройство для опечатывания);

Таблица 5 – Смета и условные обозначения СЗИ

СЗИ	Условное обозначение	Цена, руб	Количество, шт	Стоимость, руб
Усиленные звукоизоляционные двери Phoenix		89,990	6	539,940
Звукоизоляционная отделка помещений Шуманет Комби		390	15	5850
Рулонные шторы Роллайт 2 с технологией BlackOut		3,190	8	25,520
Генераторы-акустоизлучатели СА-4Б1		7,440	22	163,680
Генераторы-вибровозбудители СВ-4Б (стены)		7,440	21	156,240
Генераторы-вибровозбудители СВ-4Б (пол, потолок)		7,440	12	89,280

Генераторы-вибровозбудители СВ-4Б (двери, окна)		7,440	15	111,600
Генераторы-вибровозбудители СВ-4Б (трубопровод)		7,440	8	59,520
Блок электропитания и управления «Соната-ИП 4.3»		21,600	1	21,600
Размыкатель «Соната-ВК 4.1»		6,000	1	6,000
Размыкатель «Соната-ВК 4.2»		6,000	1	6,000
Размыкатель «Соната-ВК 4.3»		6,000	1	6,000
Средство активной защиты информации от утечки за счет ПЭМИН «Соната-РЗ»		97,200	1	97,200
Пульт управления «Соната-ДУ 4.3»		7,680	1	7,680
Генератор шума «Соната-РС2»		23,600	1	23,600
Итого				1,337,710

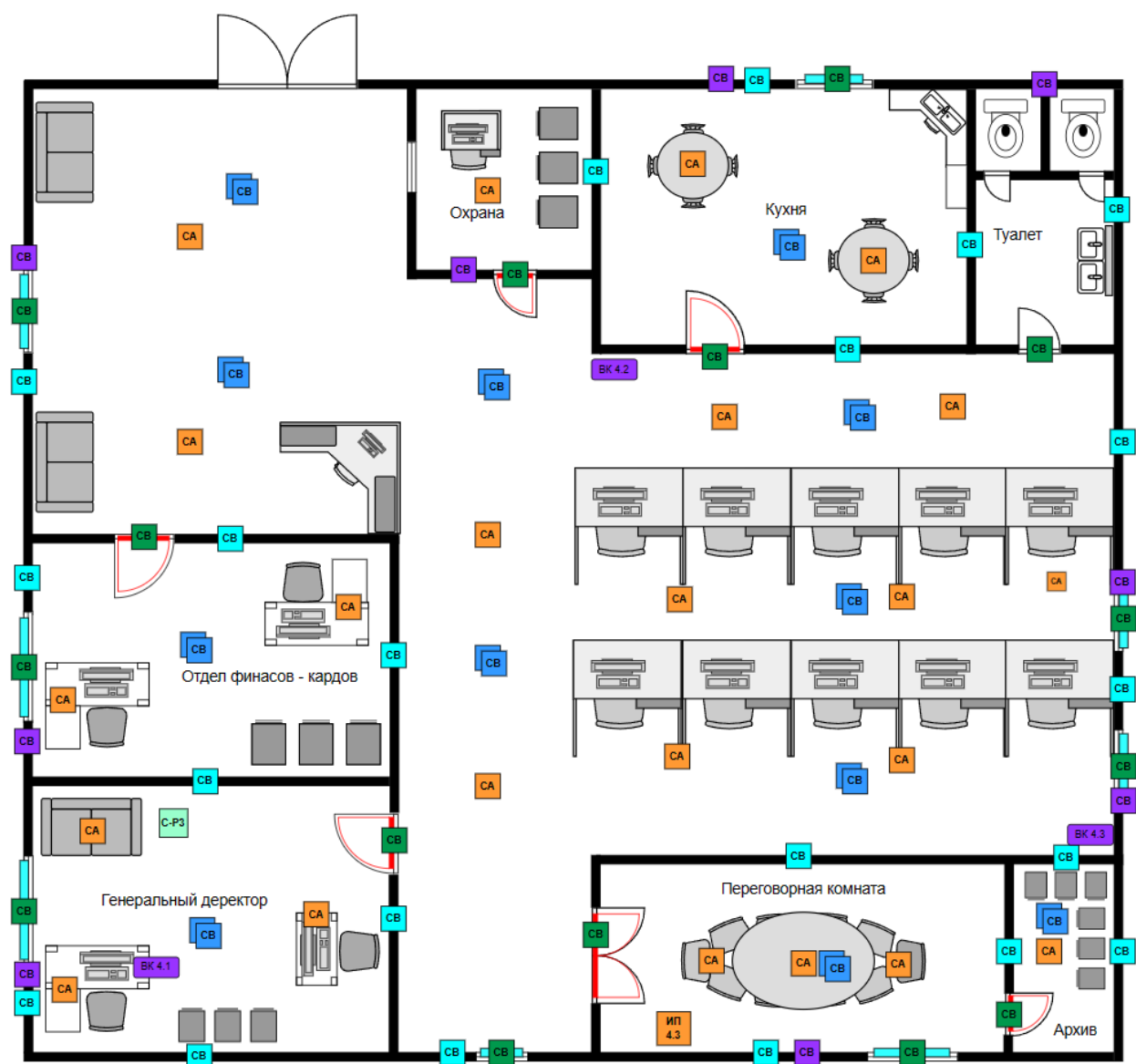


Рисунок 5 – План помещений с внедренными СИ

Пассивная защита

Было решено установить 6 усиленные двери, 8 рулонных штор на каждое окно в каждое помещение. Также была использована звукоизоляционная отделка для 4 помещений, необходимо выделить 15 рулон отделки.

Активная защита

Соната «АВ» 4Б содержит генераторы-акустоизлучатели СА-4Б1 и генераторы-вибровозбудители СВ-4Б.

1) Генераторы-акустоизлучатели СА-4Б1 – один на каждый вентиляционный канал или дверной тамбур; – один на каждые 8...12 м³ надпотолочного пространства или др. пустот.

2) Генераторы-вибровозбудители СВ-4Б

- 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;
- один на окно (при установке на оконный переплет);
- 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.

3) Блок электропитания и управления «Соната-ИП 4.3» устанавливается в количестве 1 шт. на 1-15 генераторных блока для управления одной системой защиты для выбранных помещений.

4) Размыкатели слаботочных линий "Соната-ВК4.1" предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям, "Соната-ВК4.2" по соединительным линиям систем оповещения и сигнализации, а "Соната-ВК4.3" по линиям компьютерных сетей.

5) Пульт управления «Соната-ДУ 4.3» 1 шт. для всей системы.

6) Генератор шума «Соната-РС2» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.

7) Средство активной защиты информации от утечки за счет ПЭМИН «Соната-РЗ»

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы был проведен обширный теоретический обзор существующих каналов утечки информации, а также был проведен анализ потенциальных путей утечки данных в защищаемом помещении. Необходимые меры по их защите были описаны и подробно рассмотрены. Осуществлен также анализ рынка существующих технических средств, предназначенных для противодействия выявленным каналам утечки информации, и выбраны наиболее подходящие средства защиты, соответствующие требованиям объекта.

Кроме того, был разработан и представлен план установки указанных средств, а также был произведен расчет затрат, необходимых для осуществления данного проекта. В результате выполненных работ была предложена комплексная система защиты от утечек информации через различные технические каналы, такие как акустический, виброакустический, оптический, акустоэлектрический, электрический, электромагнитный, оптико-электронный. Кроме того, достигнута защита от потенциальных угроз, связанных с ПЭМИН (поименное отключение и наведение помех). Полученные меры обеспечивают высокий уровень безопасности и защиты информации от возможных утечек в пределах рассматриваемого объекта.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Грибунин В.Г. «Комплексная система защиты информации на предприятии»
 , Академия, 2009 г
2. А. Торокин: «Инженерно-техническая защита информации: учебное пособие
 для студентов», М.: Гелиос АРВ, 2005. – 960 с.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1.
 Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320
 с.
4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации
 техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО,
 2012. - 416 с. - экз