

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

Факультет безопасности информационных технологий

Дисциплина:

«Организация и управление службой информационной безопасности»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Мониторинг сетевого трафика как способ обнаружения злоумышленников при обеспечении
информационной безопасности»

Выполнил:

студент группы N34511

Полевцов Артем Сергеевич



(подпись)

Проверил:

доцент ФБИТ, кандидат технических наук

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	Полевцов Артем Сергеевич <hr/> (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич <hr/> (Фамилия И.О)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической защиты на предприятии
Задание	<hr/> <hr/>

Краткие методические указания

Содержание пояснительной записки

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент

23.11.2023

(Подпись, дата)

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

Студент	Полевцов Артем Сергеевич
	(Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич
	(Фамилия И.О)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической защиты на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Заполнение задания на курсовую работу	30.09.2023	29.09.2023	
2.	Анализ информации	10.10.2023	12.10.2023	
3.	Написание курсовой работы	15.10.2023	26.10.2023	
4.	Подготовка презентации	25.10.2023	09.11.2023	
5.	Защита курсовой работы	09.11.2023	09.11.2023	

Руководитель

(Подпись, дата)

Студент

23.11.2023



(Подпись, дата)

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

Студент	Полевцов Артем Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической защиты на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	Цель работы: разработать комплекс инженерно-технической защиты информации, составляющей государственную тайну и персональные данные сотрудников и клиентов.
Задачи:	<ol style="list-style-type: none">1. Произвести анализ технических каналов утечки информации;2. Составить перечень управляющих документов;3. Произвести анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;4. Произвести анализ рынка технических средств защиты информации разных категорий;5. Разработать схемы расстановки выбранных технических средств в защищаемом помещении.
2. Характер работы	Отчетная курсовая работа

3. Содержание работы

1) Цель курсовой работы;

2) Задачи, решаемые в ходе выполнения лабораторной работы;

3) Организационная структура предприятия;

4) Анализ технических каналов утечки информации;

5) Анализ выбранных помещений;

6) Обоснование секретности;

7) Описание помещения;

8) Анализ технических каналов утечки информации и выбор средств защиты;

9) Анализ технических средств защиты информации;

10) Устройства для перекрытия акустического и виброакустического каналов утечки информации;

11) Защита от ПЭМИН;

12) Защита от утечек по оптическому каналу;

13) Описание расстановки технических средств защиты информации;

4. Заключение;

Руководитель

(Подпись, дата)

Студент

23.11.2023



(Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
ПОСТАНОВКА ЗАДАЧ.....	8
1.1 Цель курсовой работы.....	8
1.2 Задачи, решаемые в ходе выполнения лабораторной работы	8
ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ	9
2.1 Организационная структура предприятия	9
2.2 Анализ технических каналов утечки информации	10
2.3 Анализ выбранных помещений	16
2.3.1 Обоснование секретности	16
2.3.2 Описание помещения	18
2.4 Анализ технических каналов утечки информации и выбор средств защиты.....	24
2.5 Анализ технических средств защиты информации.....	25
2.5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации.....	26
2.5.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	29
2.5.3 Защита от ПЭМИН	31
2.5.4 Защита от утечек по оптическому каналу	33
2.6 Описание расстановки технических средств защиты информации.....	34
ЗАКЛЮЧЕНИЕ	38
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....	39

ВВЕДЕНИЕ

С течением времени и развитием технологий растет не только объем передаваемой информации, но и уровень угроз ее безопасности. За историческими перипетиями мы видим множество случаев утечек данных, которые приводили к серьезным негативным последствиям для их владельцев. В современном мире, где информация передается через разнообразные каналы связи, актуальность проблемы ее защиты становится более критической.

Необходимость эффективной защиты информации важна не только на уровне индивида, но и в контексте государственной безопасности. Слабость в защите каналов связи предоставляет потенциальным нарушителям доступ к ценной информации, что может иметь катастрофические последствия. Для противостояния таким ситуациям широко используются технические средства, которые предотвращают нежелательное распространение данных за пределы контролируемой зоны. Эти каналы, в которых возможна утечка информации, получили название "каналов утечки информации".

Настоящая работа посвящена процессу разработки комплекса инженерно-технической защиты информации с уровнем секретности "секретно" на объекте информатизации. Объект защиты включает семь помещений, охватывая офис предприятия с кабинетом директора, переговорной, рабочим кабинетом, местом для отдыха, архивом, уборной и прихожей. Структура работы включает анализ технических каналов утечки, перечень управляющих документов, анализ защищаемых помещений и разработку схем расстановки технических средств в защищаемом помещении.

ПОСТАНОВКА ЗАДАЧ

1.1 Цель курсовой работы

Целью курсовой работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну и персональные данные сотрудников и клиентов.

1.2 Задачи, решаемые в ходе выполнения лабораторной работы

1. Произвести анализ технических каналов утечки информации;
2. Составить перечень управляющих документов;
3. Произвести анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;
4. Произвести анализ рынка технических средств защиты информации разных категорий;
5. Разработать схемы расстановки выбранных технических средств в защищаемом помещении.

ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ

2.1 Организационная структура предприятия

Наименование организации: ООО “Ключ”. Область деятельности:
Государственное агентство управления недвижимостью.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа: государственная тайна, персональные данные.

Содержит информацию о государственной политике использования недвижимости, включая правила и регулятивные положения, которые определяют, как и для каких целей может использоваться государственная недвижимость. Данная информация представляет из себя государственную тайну.

- Директор Агентства (1 человек)
- Заместитель Директора (1 человек)
- Отдел Управления Недвижимостью (20 человек)
 - Руководитель отдела (1 человек)
 - Специалисты по управлению недвижимостью (19 человек)
- Отдел Юридического Обеспечения (10 человек)
 - Руководитель отдела (1 человек)
 - Юристы (9 человек)
- Отдел Финансов (10 человек)
 - Руководитель отдела (1 человек)
 - Финансовые аналитики и бухгалтеры (9 человек)
- Отдел Информационных Технологий (5 человек)
 - Руководитель отдела (1 человек)
 - IT-специалисты (4 человек)
- Отдел Кадров (5 человек)
 - Руководитель отдела (1 человек)
 - Специалисты по работе с персоналом (4 человек)

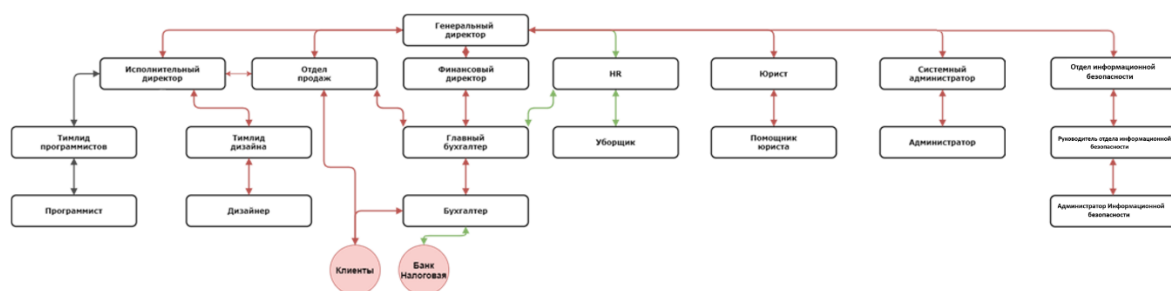


Рисунок 1 – Информационные потоки между отделами предприятия и структура организации

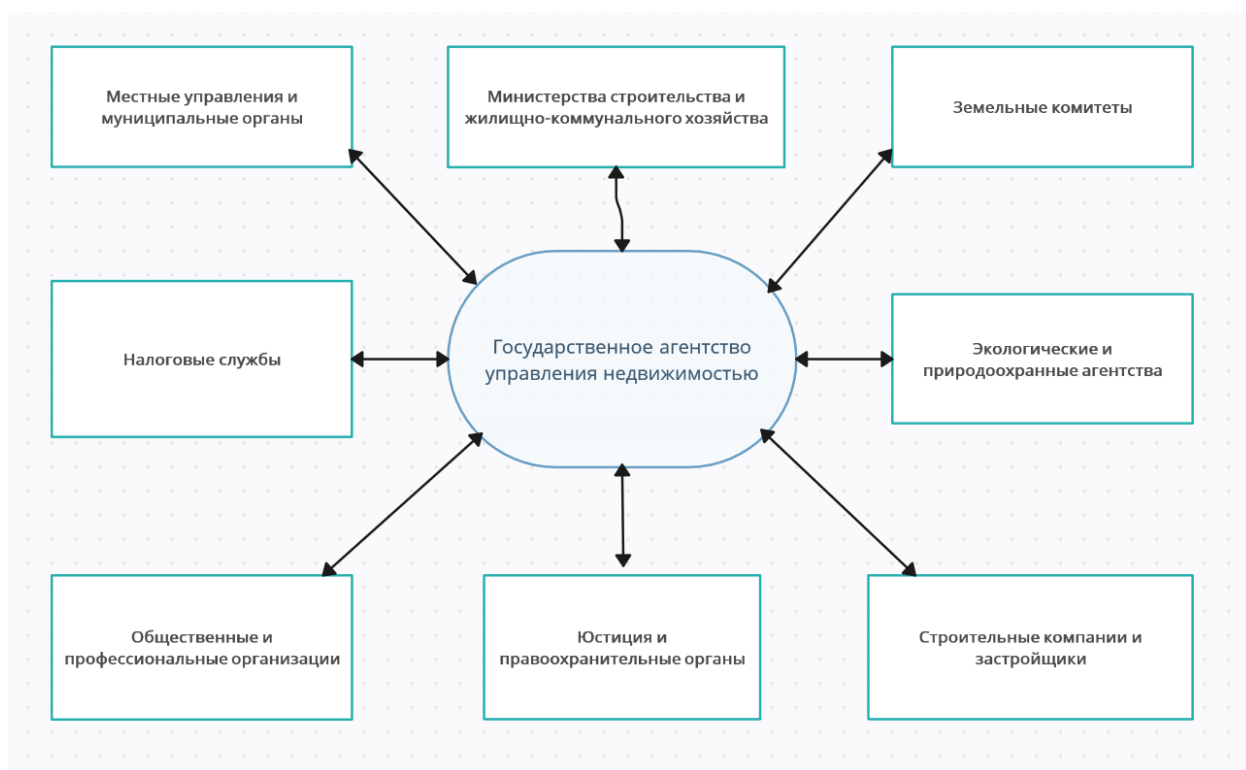


Рисунок 2 – Внешние информационные потоки

2.2 Анализ технических каналов утечки информации

Утечка конфиденциальной информации — неконтролируемый выход конфиденциальных сведений за пределы компании или круга лиц, которым доверили хранение информации ограниченного круга лиц. Утечка происходит по каналам передачи данных. Неконтролируемые каналы нарушают безопасность систем защиты.

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 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 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 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.

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 акустоэлектрическим, 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 помещении звуковую информацию. Защита осуществляется посредством использования специальных фильтров 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 твердых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технических устройств, 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.

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.

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 внимание 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.

2.3 Анализ выбранных помещений

2.3.1 Обоснование секретности

Объектом защиты является государственное агентство управления недвижимостью, которое содержит государственную тайну и персональные данные. Основным видом деятельности организации по ОКВЭД является «68.32 Управление эксплуатацией недвижимого имущества за вознаграждение или на договорной основе».

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».

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)	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
Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
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

Таблица 1 – Классы защищенности автоматизированных систем

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

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

2. совершенно секретных: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Соответственно, в рассматриваемом государственном агентстве управления недвижимостью – содержится государственная тайна, а именно, секретные сведения 3-го уровня, так как в нем обрабатывается секретная государственная информация.

2.3.2 Описание помещения

Перед тем, как перейти к разработке комплекса инженерно-технической защиты информации, необходимо описать выбранные помещения.

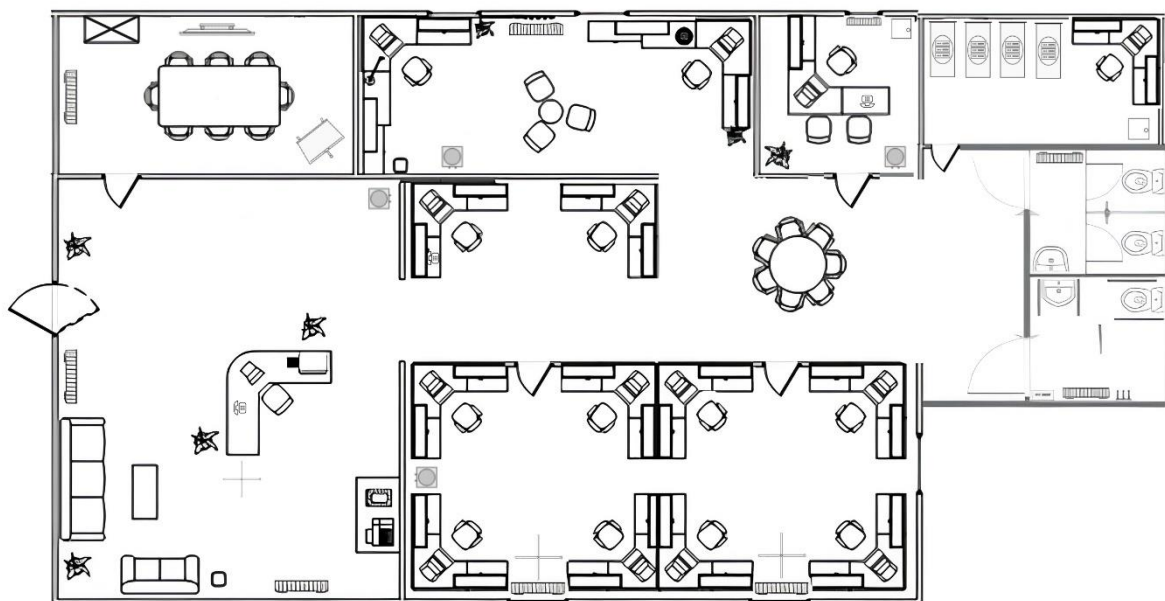


















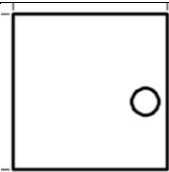



Рисунок 3 - План помещения

Обозначение	Название
 	Диваны
	Рабочие кресла
	Стулья
	Урна для мусора
	Персональный Компьютер
	Кофейный стол
	Журнальный стол

	Комнатное растение
	Шкаф для книг
	МФУ
	Пресс-папье
	Батарея центрального отопления
	Принтер
	Умывальник
	Санузел
	Вешалка
	Городской телефон
	Сейф
	Кулер с водой


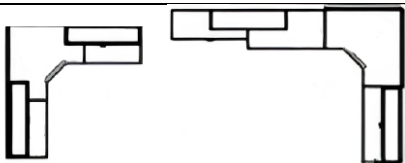
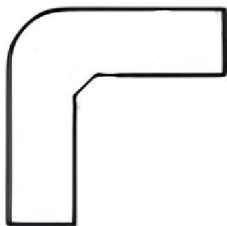



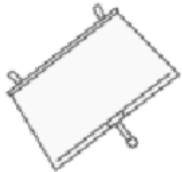

	Стол в переговорной
	Рабочий стол сотрудника
	Стол на ресепшн
	Чайник
	Напольная вешалка
	Большой телевизор
	Флипчарт
	Архивный шкаф

Таблица 2 - Описание элементов, изображенных на плане помещения

Рассматриваемые помещения имеют следующую площадь:

- кабинет директора: 25 м²;
- переговорная: 31,5 м²;
- архив: 23 м²;
- рабочий кабинет для четырех сотрудников 1: 30 м²;
- рабочий кабинет для четырех сотрудников 2: 30 м²;
- рабочий кабинет для двух сотрудников: 11 м²;
- пространство для отдыха: 35 м²;
- 2 санузла: 24 м²;
- зона ресепшн: 50 м²;

Для ведения переговоров предназначено одно помещение (переговорная), там находятся стол для переговоров и 8 стульев вокруг него, флипчарт, большой телевизор, одна батарея центрального отопления, книжные полки, 6 розеток.

В двух одинаковых рабочих кабинетах имеется по четыре рабочих места (стол, стул и ПК), по одному окну, по одной батарее центрального отопления, под каждым столом - урна для бумаг, по одной напольной вешалке и по 15 розеток, одна урна для мусора и горшок с комнатным растением.

В этих помещениях обрабатываются конфиденциальные данные и ведется работа с государственной тайной. Важно обеспечить, чтобы информация на экранах компьютеров не была видна из-за окон или дверей. Также следует обеспечить безопасное хранение и уничтожение любых бумажных документов.

Архив представляет из себя небольшое помещение без окон внутри - 4 архивных шкафа, одно рабочее место и сейф. Требуется наиболее строгих мер безопасности, поскольку оно содержит государственную тайну.

В пространстве для отдыха имеем 2 окна, одна батарея центрального отопления, два стола с компьютерами, два комнатных растения, пять стульев, электрический чайник, урна для мусора, кулер для воды.

Кабинет директора имеет одно окно, одну батарею, 10 розеток, два стула для посетителей, кресло рабочее, рабочее место с ПК и городским телефоном, личный сейф. Также является приоритетным местом для защиты, поскольку здесь находится компьютер директора, а также его сейф.

В рабочем кабинете для двух сотрудников находится два рабочих места (столы, стулья, компьютеры) и городской телефон.

В зоне ресепшн находится стойка ресепшн, два дивана, журнальный столик, четыре комнатных растения, две батареи, напольная вешалка, стол с компьютером для администратора, принтер, городской телефон. Отдельно стол с пресс-папье и МФУ. И один кулер с водой.

Помещение расположено на пятом этаже офисного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. Часть внутренних перегородок железобетонные, толщиной не менее 5 см, другая часть сделана из звукоизоляционного гипсокартона.

2.4 Анализ технических каналов утечки информации и выбор средств защиты

Если говорить о возможных утечках информации, то 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.

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 средствами защиты.

Каналы	Источники	Пассивная защита	Активная защита
акустический / акустоэлектрический	окна, двери, проводка	звукоизоляция переговорной, фильтры для сетей электропитания	устройства акустического зашумления
вибрационный / виброакустический	все твердые поверхности помещения, батареи	изолирующие звук и вибрацию обшивки стен	устройства вибрационного зашумления
электромагнитный / электрический	розетки, армы, бытовая техника	фильтры для сетей электропитания	устройства электро- магнитного зашумления
оптический	окна, двери	жалюзи / шторы на окнах, тонирующие пленки на окна, доводчики на дверях	бликующие устройства

Таблица 3 - Активная и пассивная защита информации

К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях

электрооборудования, защитные фильтры и т. д. 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 нарушающее нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

2.5 Анализ технических средств защиты информации

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «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 см. 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 этаже, 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 информации.

2.5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Акустический и виброакустический каналы утечки информации - это пути, по которым информация может утекать из информационной системы через звуковые и вибрационные сигналы.

Виброакустический канал состоит из объекта сигнала, среды распространения и агента, принимающего данные. Среда распространения - это не воздух, а строительные и другие конструкции, которые при прохождении акустического сигнала создают вибрацию. Эта вибрация затем снимается при помощи лазерного луча и преобразуется в информацию.

Пассивные способы защиты от утечки информации по акустическим и виброакустическим каналам могут включать использование:

- звукопоглощающих облицовочных материалов;
- специальных дополнительных тамбуров;
- дверных проемов;
- двойных оконных переплетов;

Активная защита акустического и виброакустического каналов утечки информации включает в себя использование устройств, создающих вибрационные и акустические помехи, предназначенные для обеспечения защиты речевой информации от ее утечки из помещений по строительным конструкциям и инженерно-техническим коммуникациям.

Эти устройства могут быть использованы для создания помех, которые маскируют или прерывают передачу информации через акустические и виброакустические каналы. Это может включать в себя использование устройств, которые создают фоновый шум или вибрации, чтобы затруднить перехват информации.

Устройство	Цена, руб.	Диапазон частот, Гц	Состав
	53300	60-16000	Имеет четыре канала формирования помех, к каждому из которых могут подключаться

			<p>вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха.</p>
Цифровой генератор сигналов "ЛГШ-403"	10752	не указано	<p>вибропреобразователи и акустические излучатели, подключаемые к генератору виброакустического шума от 1 до 4-х;</p> <p>генератор виброакустического шума ЛГШ-403 в комплекте с блоком питания от сети 220 В;</p> <p>акустический излучатель ЛВП-2а;</p> <p>электромагнитные вибропреобразователи ЛВП-2о для установки на окна;</p> <p>электромагнитные вибропреобразователи ЛВП-2с для установки на стены;</p> <p>электромагнитные вибропреобразователи ЛВП-2т для установки на трубы.</p>
Генератор шума ПУЛЬСАР	24525	от 10000 до 6000000000	<p>Комплекс виброакустической защиты помещения - это комплект, состоящий из</p>

			устройств СВ-4Б, СА-4Б, Соната ИП-4.3, Соната-ДУ-4.3 и набора креплений для установки
Виброакустический шумогенератор "SI-3010"	25194	125 – 6300	трехканальный прибор виброакустической защиты SI - 3010; электромагнитные излучатели TRN -2000 для формирования помехи в стенах и перекрытиях помещения; виброакустические преобразователи ВД-1 для формирования помехи в оконных стеклах, системе отопления и вентиляции помещения; акустические излучатели OMS-2000

Таблица 5 - Сравнительный анализ средств активной защиты по виброакустическому каналу

Из вышеперечисленных устройств для нашей организации будет выбрано устройство - Виброакустическая защита Генератор шума ПУЛЬСАР по ряду причин:

- Имеет диапазоны частот от 10 кГц до 6 ГГц
- 2 съемные антенны, счетчик наработки
- Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук)
- Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом)
- Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России) – по 2 классу защиты
- Можно применять в выделенных помещениях до 2 категории включительно

2.5.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

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 5 приведен сравнительный анализ подходящих средства пассивной защиты помещений по электрическому каналу.

Устройство	Цена, руб.	Состав
ЛФС-10-1Ф, Фильтр сетевой помехоподавляющий до 10А	47060	Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц «ЛФС-10-1Ф» соответствует: - типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. ЛФС-10-1Ф» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.
ФЭПС-10	42870	Для пассивной защиты конфиденциальной информации, содержащейся в побочных излучениях

		<p>вычислительной техники, рекомендуется использовать специальные фильтры.</p> <p>Одним из таких устройств является сетевой фильтр ФЭПС-10. Данный прибор имеет действующий сертификат ФСТЭК, поэтому его можно устанавливать в выделенных помещениях 3, 2 и 1 категории.</p> <p>ФЭПС-10 – 2-проводный фильтр, который предназначен для подключения к сетям без провода заземления. По техническим параметрам он рассчитан для встраивания в электроцепь с номинальным напряжением 220В, номинальной силой тока 10А и частотой 50Гц. Производитель не исключает возможности параллельного подключения 2 и более ФЭПС-10.</p> <p>Сертификат № 4282 ФСТЭК РФ</p>
<p>Фильтр сетевой помехоподавляющий ЛППФ-10-1Ф</p>	47000	<p>Устройство ЛППФ-10-1Ф предназначено для защиты информации от утечки за счет побочных электромагнитных наводок на однофазные линии электропитания.</p> <p>Устройство ЛППФ-10-1Ф может применяться для защиты объектов обрабатывающих сведения составляющие государственную тайну, а также для объектов обрабатывающих конфиденциальную информацию.</p>

Таблица 6 - Сравнительный анализ средств пассивной защиты по электрическому каналу

Наиболее подходящим фильтром для наших целей является ФЭПС-10 по следующему ряду причин:

- Имеет сертификат № 4282 ФСТЭК РФ

- Отлично подходит для пассивной защиты конфиденциальных данных от утечки по электросети
- Фильтр импульсных/высокочастотных помех, скачков напряжения
- Подходит для подключения к сети с номинальной силой тока до 10А, напряжением 220В
- Двухпроводное исполнение
- Может эксплуатироваться в выделенных помещениях всех категорий.

2.5.3 Защита от ПЭМИН

ПЭМИН - побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации.

Устройство	Цена, руб.	Состав
ЛГШ-513	39 000	Визуальная система индикации нормального режима работы; Визуально-звуковая система индикации аварийного режима (отказа); Счетчик учета времени работы в режиме формирования маскирующих помех (ЖК-дисплей); Защита органов регулировки уровня выходного шумового сигнала; Проводное дистанционное управление и контроль (через программно-аппаратный комплекс «Паутина»); Есть сертификат ФСЭК;
Покров, исполнение 2	37 500	Может применяться в выделенных помещениях до 1 категории включительно; Централизованное управление и контроль по Ethernet (для дистанционного управления или применения в системах пространственного зашумления); Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления;

		<p>Выполнен в виде сетевого удлинителя с 5 розетками типа F;</p> <p>Может быть смонтирован в 19" стойку (может заменить блок распределения питания базовый, высота 2U);</p> <p>На заказ может поставляться с вилкой IEC C14 (для подключения к ИБП).</p>
ЛГШ-516СТАФ	51000	<p>Рабочий диапазон частот прибора широк и составляет от 0,009 МГц до 6 ГГц. Для регулирования выходного сигнала есть 5 уровней. Вы можете регулировать настройки через проводное дистанционное управление и контроль (в том числе через программно-аппаратный комплекс «Паутина»). У ЛГШ-516 работает система индикации как нормального режима работы, так и визуально-звуковая система индикации аварийного режима (отказа), причем на случай аварийного отключения электроэнергии есть энергозависимая память для сохранения настроек.</p>
Соната-РЗ.1	33120	<p>комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления);</p> <p>наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений;</p> <p>возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0.01...100 МГц за счет применения опционально поставляемой дополнительной антенны;</p> <p>встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией;</p> <p>возможность удаленного управления изделием как в случае автономного использования (непосредственно Пульт-ДУ4.x), так и в случае использования в составе комплекса ТСЗИ;</p>

		наличие счетчика наработки в режиме «Излучение».
--	--	--

Таблица 7 - Сравнительный анализ средств активной защиты от ПЭМИН

Наиболее подходящий прибор для нашего помещения это ЛГШ-516СТАФ по ряду причин:

- Прибор может быть использован в целях защиты информации, содержащей сведения, составляющие государственную тайну (сертификат ФСТЭК по 2 классу защиты)
- Рабочий диапазон частот от 0,009 МГц до 6 ГГц
- Может устанавливаться в ВП до 2 категории включительно
- 5 уровней регулировки выходного сигнала
- Время непрерывной работы не менее 12 часов

2.5.4 Защита от утечек по оптическому каналу

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

Возможность наблюдения объектов определяется величиной падающего потока света (освещенность), отраженного от объекта света (отражающие свойства) и контрастом объекта на фоне окружающих его предметов. Днем (освещенность создается Солнцем) глаз человека обладает наибольшей цветовой и контрастной чувствительностью. В сумерки освещенность постепенно падает. Уменьшение освещенности вызывает ухудшение работы зрения, а следовательно, сокращение дальности и ухудшение цветоразличия. Эти физические особенности необходимо учитывать при защите информации от утечки по визуально-оптическим каналам.

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- использовать средства преграждения или значительного ослабления отраженного света: ширмы, шторы, ставни, темные стекла, преграды;
- применять средства маскирования, имитации и другие с целью введения в заблуждение злоумышленника;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;

- применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

2.6 Описание расстановки технических средств защиты информации

Согласно информации, приведённой в предыдущих пунктах, выбранные средства защиты информации включают в себя:

- усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 3 шт., в переговорную, архив и кабинет директора;
- генератор шума ПУЛЬСАР;
- устройство пассивной защиты от ПЭМИН ЛГШ-516СТАФ;
- 5 комплектов жалюзи на 5 окон;
- доводчики на 5 дверей.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. Согласно руководству по эксплуатации «Система виброакустической и акустической защиты Соната АВ-4Б. Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

- 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.

Ориентировочное количество пьезоизлучателей может быть определено из расчета: один ПИ-45 на каждое стекло.

Необходимое количество аудиоизлучателей можно предварительно оценить из следующих норм:

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

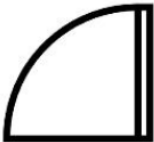
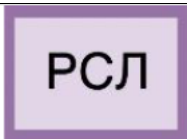
Основным правилом, которым следует руководствоваться при выборе мест установки излучателей в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации при обеспечении приемлемого уровня мешающего акустического

шума в защищаемом помещении. Контроль вибрационного и акустического зашумления помещений рекомендуется производить в соответствии с методиками и рекомендациями ФСТЭК (Гостехкомиссии) РФ.

Средство защиты	Цена, руб.	Количество, шт.	Количество, шт
Генератор-акустоизлучатель "СА-4Б"	7440	18	133920
Вибровозбудители "Соната-СВ-4Б"	7440	53	394320
Соната ИП-4.3	21600	1	21600
Пульт управления Соната-ДУ 4.3	7680	1	7680
ЛГШ-516СТАФ	51000	1	51000
ФЭПС-10	42870	1	42870
Дверь со звукоизоляцией	80000	5	400000
Генератор шума ПУЛЬСАР	24525	1	24525
Жалюзи	3105	5	15525
Итого:	1091440		

Таблица 8 - Смета затрат на выбранные средства защиты информации

Жалюзи установлены на каждом окне, а доводчики на каждой двери. Элементы комплексной системы Соната «АВ» модель 4Б расположены так же, как и на рисунке. ЛГШ-516СТАФ подключен напрямую к «Соната-ИП4.3» и на схеме отдельно не обозначена. «ПУЛЬСАР» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.

Средство защиты	Условное обозначение	Количество, шт.
Дверь звукоизолирующая		5
Размыкатель слаботочной линии		1

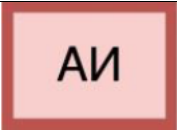

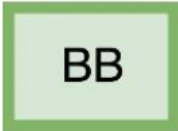

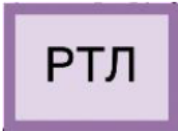
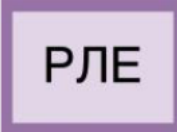


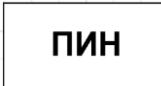
«Соната-СА-4Б» генератор-акустоизлучатель		18
Блок электропитания и управления «Соната-ИП4.3»		1
«Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок)		14
«Соната-СВ-4Б» генератор-вибровозбудитель (трубопровод)		5
Размыкатель телефонной линии		1
Размыкатель линии Интернета		1
«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна, батареи)		20
«Соната-СВ-4Б» генератор-вибровозбудитель (стены)		14
ЛГШ-516СТАФ		1

Таблица 9 - Условные обозначения схемы расстановки устройств

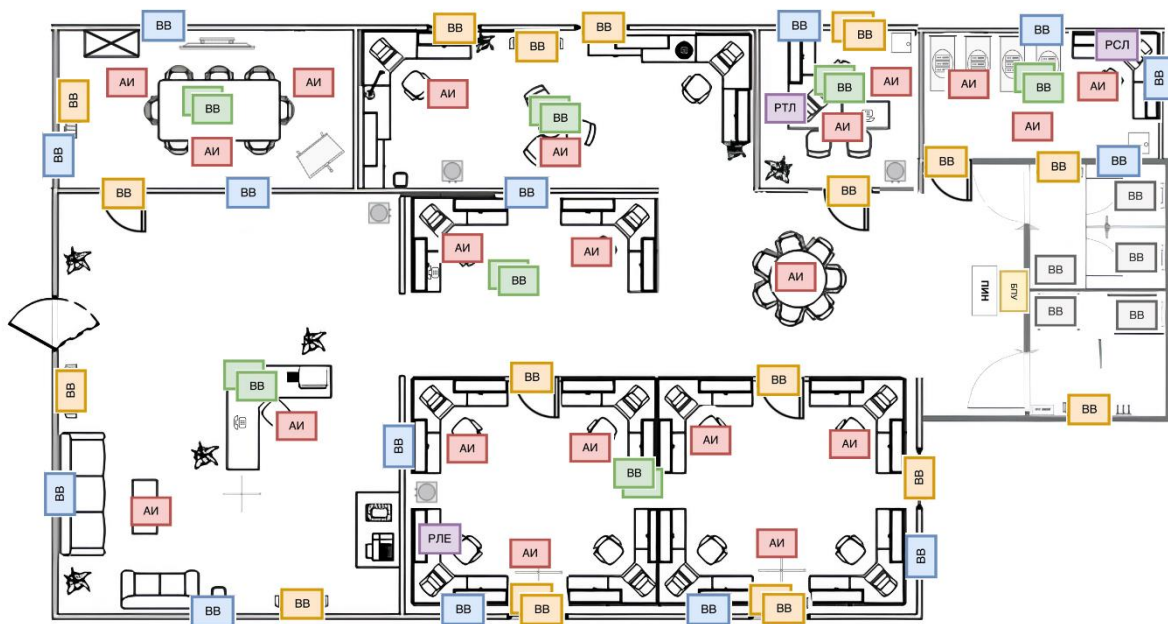


Рисунок 2 - Схема расстановки устройств

ЗАКЛЮЧЕНИЕ

В процессе выполнения данного исследования проведен тщательный теоретический анализ технических каналов, через которые возможна утечка информации. Затем были выявлены ключевые руководящие документы, осуществлен детальный анализ помещений, подлежащих защите, проведена оценка потенциальных каналов утечки информации, и выбраны эффективные меры как пассивной, так и активной защиты данных.

В итоге была разработана смета на основе текущих цен на технические средства для обеспечения информационной безопасности. Общая сумма затрат оценена в 1091440 рублей. Также была разработана детальная схема размещения устройств для максимально эффективной защиты информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждено 30.08.2002 приказом Председателя Гостехкомиссии России No 282.
2. ГОСТ Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения».
3. Руководящий документ Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.
4. «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» - Москва.
5. Решение Межведомственной комиссии по защите государственной тайны от 21 января 2011 г. N 199 "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".
6. Detector System. Средства защиты переговоров [HTML] (https://detsys.ru/catalog/sredstva_zashchity_peregovorov/) (Дата обращения: 18.12.2022).