

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

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

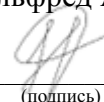
«Проектирование системы защиты от утечки информации по различным каналам.

Вариант 9»

Выполнила:

студент группы N34461

Нуртдинов Альфред Арсенович



(подпись)

Проверил:

доцент факультета БИТ, к.т.н

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	Нуртдинов А.А. <div>(Фамилия И.О)</div>
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов И.Ю. <div>(Фамилия И.О)</div>
Должность, ученое звание, степень	Доцент факультета БИТ, к.т.н.
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации по различным каналам. Вариант 9
Задание	Спроектировать систему защиты от утечки информации по различным каналам

Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
2. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы.
4. Краткая характеристика организации.
5. Анализ защищаемых помещений.

6. Анализ рынка инженерно-технических средств.

7. Разработка инженерно-технической системы защиты информации..

8. Заключение.


9. Список литературы.

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент


 25.12.2023

(Подпись, дата)

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

Студент	Нуртдинов А.А.
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов И.Ю.
	(Фамилия И.О.)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации
	по различным каналам. Вариант 9

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	05.10.2023	05.09.2023	
2.	Анализ теоретической составляющей	11.11.2023	11.11.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	18.12.2023	18.12.2023	
4.	Представление выполненной курсовой работы	25.12.2023	25.12.2023	

Руководитель	
	(Подпись, дата)
Студент	 25.12.2023
	(Подпись, дата)

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

Студент	Нуртдинов А.А.
	(Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов И.Ю.
	(Фамилия И.О)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации
	по различным каналам. Вариант 9

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
2. Характер работы	Конструирование
3. Содержание работы	
	1. Введение.
	2. Анализ технических каналов утечки информации.
	3. Руководящие документы.
	4. Краткая характеристика организации.
	5. Анализ защищаемых помещений.
	6. Анализ рынка технических средств.
	7. Описание расстановки технических средств.
	8. Заключение.

9. Список литературы.

4. Выводы

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

Руководитель

(Подпись, дата)

Студент

25.12.2023

(Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	8
1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ	9
1.1 Электрические и электромагнитные каналы утечки информации	10
1.2 Акустические каналы утечки информации	11
1.3 Визуально-оптические каналы утечки информации	12
1.4 Материально-вещественный канал утечки информации	14
2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ	15
3 ИНФОРМАЦИОННЫЕ ПОТОКИ	17
4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	19
4.1 Описание защищаемых помещений	19
4.2 Анализ возможных каналов утечки информации	20
5 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	21
5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации	21
5.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	22
5.3 Защита от ПЭМИН	23
5.4 Защита от утечек по визуально-оптическому каналу	26
6 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	28
ЗАКЛЮЧЕНИЕ	29
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	30

ВВЕДЕНИЕ

Деятельность любого современного предприятия основана на обладании и управлении информацией. В связи с этим защита информации становится предметом пристального внимания, так как повсеместно внедряемые технологии и компоненты без соответствующих предосторожностей быстро становятся источниками проблем.

Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию. Разработка эффективного комплекса мер для выполнения данной задачи является одной из наиболее актуальных современных проблем. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из восьми помещений и представляет собой офис предприятия со следующими помещениями: кабинет директора, комната отдыха, туалет, кухня, компьютерный зал, серверная, переговорная.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов. В третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий. Пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечкой информации считают неправомерное распространение набора сведений, выходящее за пределы круга доверенных лиц или организаций, которые хранили эти сведения. Утечкой называют противоправное овладение чужой информацией вне зависимости от того, каким способом достигается получение данных.

Утечка информации происходит при сопутствующих условиях, которые допускают ее возникновение:

- некомпетентность сотрудников, которые занимаются защитой данных, их непонимание важности процесса и халатное отношение к информации;
- использование нелегальных средств или не прошедших сертификацию программ по защите конфиденциальной информации;
- низкая степень контроля над средствами охраны сведений;
- постоянная смена сотрудников, которые занимаются защитой конфиденциальной информации.

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

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации, оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы, такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

Канал утечки данных, которыми владеет компания, может быть физическим, техническим или информационным. В рамках курсовой работы рассматривается только технический канал.

Техническим называют канал, в котором источниками информации служат шумовые

сигналы, излучения и вибрации, исходящие от интересующих объектов. Распространение сигналов происходит через определенную физическую среду (волновую или электрическую).

Технический канал утечки информации (ТКУИ) представляет собой комплексный набор элементов, включая объект технической разведки, физическую среду, через которую распространяется информативный сигнал, а также средства, используемые для добывания защищаемой информации. Утечка информации через технический канал представляет собой неконтролируемый процесс распространения информации от источника защищаемой информации через физическую среду до технического устройства, осуществляющего перехват этой информации. Структура технического канала утечки информации представляет из себя два основных компонента - источник и злоумышленник. Между ними расположен канал утечки информации, состоящий из источника сигнала, среды по которой передается сигнал и приемника.

Информация, поступающая от источника, начинает свой путь через канал, используя язык источника. Для того чтобы записать эту информацию на носитель, соответствующий среде распространения, передатчик осуществляет ее преобразование в форму, соответствующую условиям данной среды.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида — твердые, жидкие, газообразные).

Каждому виду каналов утечки информации свойственны свои специфические особенности.

1.1 Электрические и электромагнитные каналы утечки информации

К электромагнитным относятся каналы утечки информации, возникающие за счёт различного вида побочных электромагнитных излучений и наводок (ПЭМИН) технических средств приема, обработки, хранения и передачи информации:

- излучений элементов технических средств приема, обработки, хранения и передачи информации;

- излучений на частотах работы высокочастотных генераторов технических средств приема, обработки, хранения и передачи информации;
- излучений на частотах самовозбуждения усилителей низкой частоты технических средств приема, обработки, хранения и передачи информации.

Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1—0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые — наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

Электрические каналы утечки информации возникают за счёт:

- наводок электромагнитных излучений технических средств приема, обработки, хранения и передачи информации на соединительные линии вспомогательных технических средств и систем и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивания информационных сигналов в линии электропитания и цепи заземления технических средств приема, обработки, хранения и передачи информации;
- использования закладных устройств для съема информации.

1.2 Акустические каналы утечки информации

Акустические технические каналы утечки информации делятся на акустоэлектрическом, виброакустическом и акустические.

Акустоэлектрический канал основан на воздействии звуковых волн на электрические устройства. Например, звуковые колебания, создаваемые при разговоре, могут воздействовать на электронику, и такие изменения могут быть перехвачены для извлечения информации.

Виброакустический канал использует вибрации, созданные на поверхности объекта, для передачи информации. Например, вибрации стекла окна, вызванные разговором, могут быть обнаружены и интерпретированы для утечки информации.

Акустический канал основан на передаче звуковых волн для утечки информации. Например, запись звука среды может содержать разговоры или другую конфиденциальную информацию.

Съемными устройствами являются стетоскопы, контактные микрофоны, способные получать и преобразовывать получаемую в виде механических колебаний информацию в акустический сигнал. Преобразования происходят в два этапа: сначала данные переводятся в формат электромагнитных колебаний, затем в акустическую информацию. Преобразования не всегда дают полностью разборчивый текст, но ряд сведений можно получить путем программного восстановления смысла по контексту. Для съема данных иногда используются лазерные лучи. Наиболее часто они применяются для отражающих свет элементов коммуникаций, стекол окон и переговорных комнат.

Съемное устройство может быть установлено на перегородку со стороны соседнего офиса или на трубу в помещении котельной. Поиск затрудняется из-за невозможности свободно проводить обследования помещений, принадлежащих другим собственникам. Для установки устройства иногда не нужен и физический контакт с проводником виброакустической информации, он может быть направлен в место установки выстрелом из специального пистолета.

Организационно-технические меры подразделяются на активные(звукоизоляция, звукопоглощение) и пассивные(звукоподавление, защищенные акустические системы).

Защита от утечки по акустическим каналам реализуется:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического зашумления объемов и поверхностей;
- закрытием вентиляционных каналов, систем ввода в помещения отопления, электропитания, телефонных и радиокommunikаций;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки информации.

1.3 Визуально-оптические каналы утечки информации

Оптические каналы утечки информации основаны на использовании световых сигналов для передачи данных. Существуют три основных вида: инфракрасный, видимый и ультрафиолетовый каналы. Инфракрасный канал использует инфракрасные световые волны для передачи данных. Например, инфракрасные сигналы, передаваемые между устройствами, могут быть перехвачены для получения конфиденциальной информации. Видимый канал использует световые волны видимого спектра для передачи данных. Например, световые мигания на экране могут быть использованы для передачи информации, которая может быть зафиксирована визуально или с помощью оптических устройств.

Ультрафиолетовый канал использует ультрафиолетовые световые волны для передачи данных. Например, ультрафиолетовые метки на документе могут быть использованы для скрытой передачи информации, которую можно раскрыть с помощью специальных оптических устройств.

По способу перехвата информации визуально-оптические технические каналы утечки информации подразделяют на оптические каналы:

- визуального наблюдения (невооруженным глазом или через бинокль);
- фотографирования и видеосъемки;
- перехвата видимого и ИК-излучения, исходящего от объекта информации, с помощью скрытно установленных датчиков.

С целью защиты информации от утечки по оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;
- 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.

1.4 Материально-вещественный канал утечки информации

В материально-вещественном канале утечки информации, нарушение конфиденциальности данных происходит путем неправомерного распространения информации за пределы контролируемой зоны вещественных носителей. В данном контексте вещественными носителями являются часто используемые материалы, такие как черновики документов и использованная копировальная бумага, а также портативные устройства хранения данных, такие как жесткие диски (HDD), твердотельные накопители (SSD), и карточки памяти.

В рамках курсовой работы не рассматривается данный канал, так как кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

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 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
- Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных».
- 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»
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
- Межведомственная комиссия по защите государственной тайне решение № 199 от 21.01.2011 г.
- "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

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

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.
- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.

- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.
- Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 ИНФОРМАЦИОННЫЕ ПОТОКИ

Схематичная структура Общества представлена на рисунке 1.

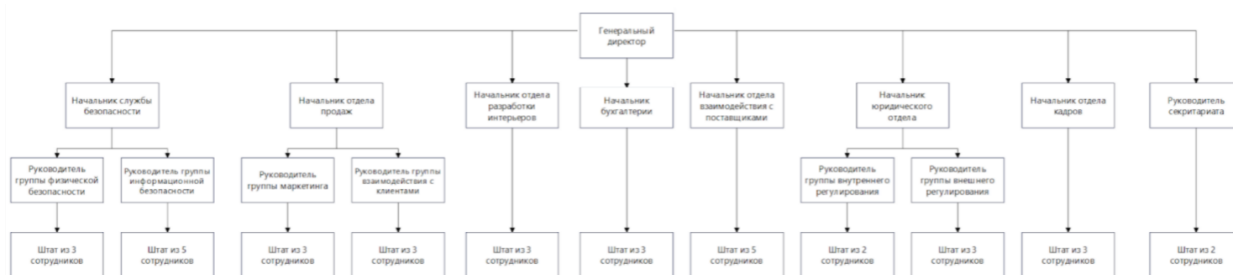


Рисунок 1 - Структура организации

В организации обрабатывается информация конфиденциального характера:

- персональные данные;
- сведения, отнесенные к коммерческой тайне организации, включающие в себя деловые секреты, финансово-экономическую, технологическую информацию, технологические секреты организации (ноу-хау), сведения, содержащиеся в служебной документации Общества, кроме официально публикуемых, идеи и разработки, полученные сотрудниками в процессе трудовой деятельности;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Также в информации обрабатываются сведения, составляющие государственную тайну с грифом "секретно", поскольку Общество также осуществляет разработку интерьеров и проектирует маскирующие дизайнерские решения для Кремля и других правительственных учреждений с целью сокрытия мест хранения документов, сейфов и секретных комнат. К таким сведениям относятся:

- планы и схемы помещений в Кремле, включая расположение комнат, коридоров, их размеры и функциональное назначение;
- детали безопасности, такие как расположение секретных комнат, сейфов и мест для хранения документов;
- спецификации и технические характеристики оборудования, используемого в интерьерах Кремля;
- информация о системах безопасности и контроля доступа к Кремлю;
- непосредственно сами разрабатываемые дизайнерские решения, включая цветовые схемы, материалы и мебель, используемые в интерьерах.
- любые сведения о том, какие особенные меры принимаются для обеспечения безопасности и конфиденциальности внутри Кремля;

- любая информация, которая может подвергнуть опасности безопасность Кремля и государственных органов, если она попадет в ненадежные руки.

Информационные потоки организации представлены на рисунках 2 и 3.

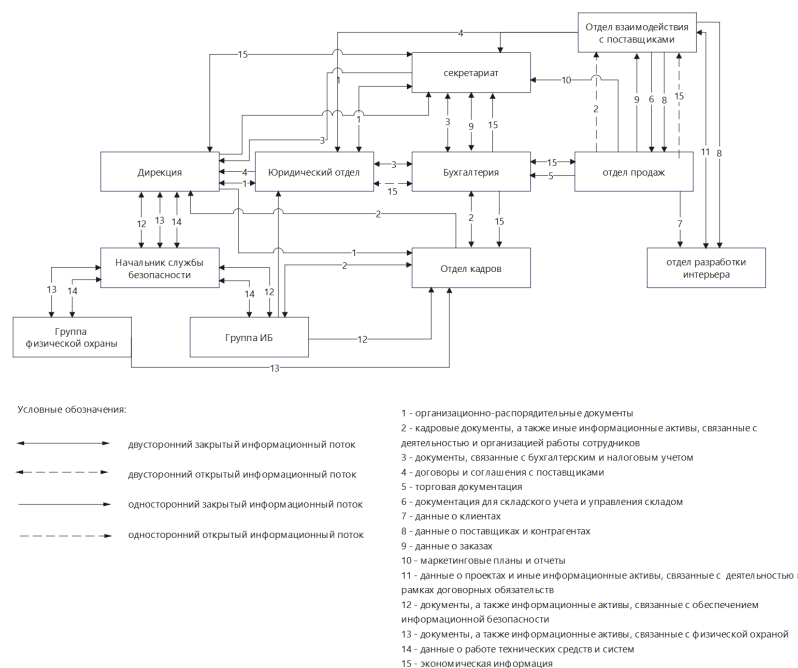


Рисунок 2 - Внутренние информационные потоки организации

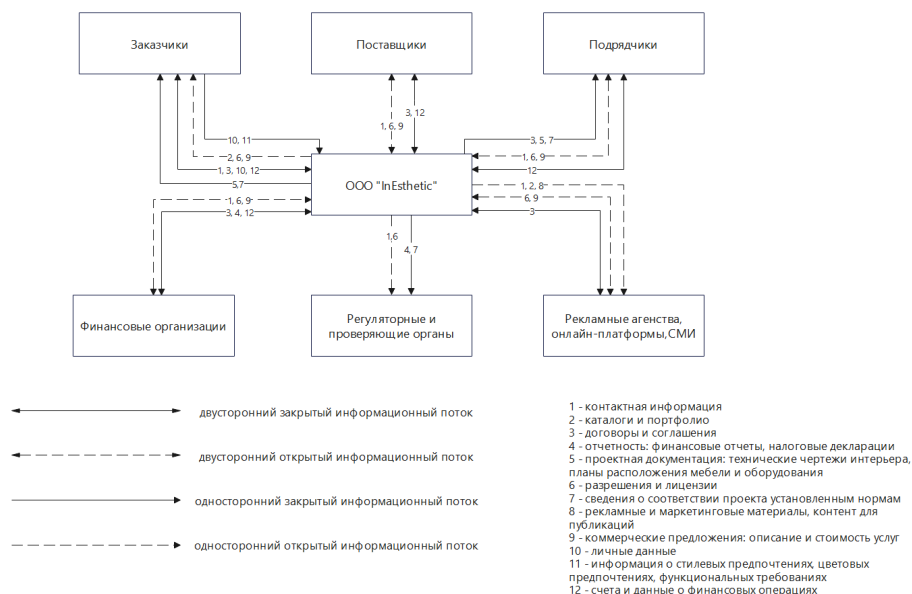


Рисунок 3 - Внешние информационные потоки организации

4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

4.1 Описание защищаемых помещений

Анализ защищаемых помещений приведён на рисунке 4.

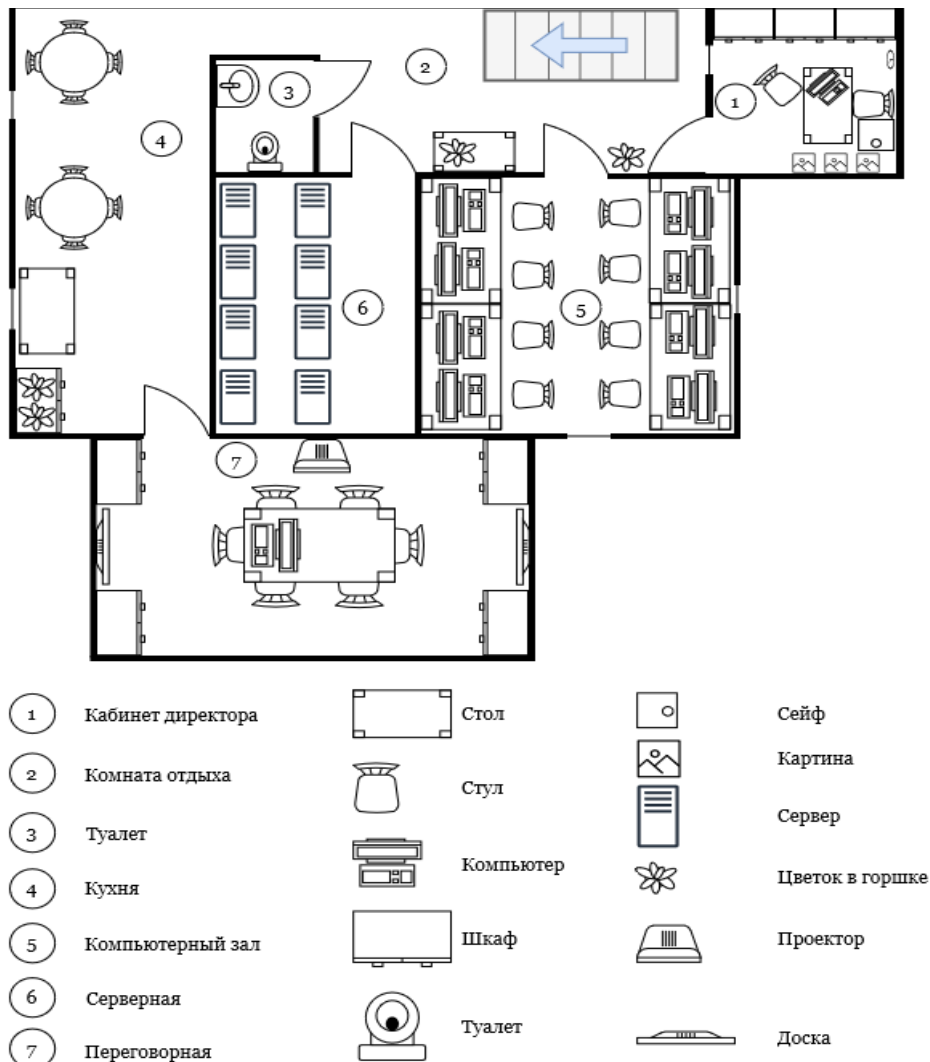


Рисунок 4 – План защищаемого помещения

Защите подлежат следующие помещения:

- кабинет директора, 5 м × 4 м (20 м²);
- серверная, 5 м × 8 м (40 м²);
- переговорная, 10 м × 6 м (60 м²);
- компьютерный зал, 8 м × 8 м (48 м²).

В кабинете директора расположены: стол, компьютер, 3 шкафа, 3 портрета, металлический сейф и часы. В помещении есть окно.

В серверной имеются 8 компьютеров. В помещении нет окон.

В переговорной находятся: большой стол, 4 шкафа, 2 доски, проектор и компьютер. В помещении нет окон.

В компьютерном зале расположены 4 стола и 8 компьютеров. В помещении 2 окна.

Офис расположен на третьем этаже трёхэтажного 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.

4.2 Анализ возможных каналов утечки информации

В помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрический и электромагнитный каналы 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 средствам защиты, приведенными в таблице 1.

Таблица 1 – Активная и пассивная защита информации

Канал утечки	Источник	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка	Звукоизоляция переговорной, фильтры для сетей электропитания	Устройства акустического зашумления
Вибрационный, виброакустический	Все твердые поверхности помещения, батареи	Дополнительное помещение перед переговорной, изолирующие звук и вибрацию обшивки стен	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного зашумления

5 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой усиленные двери, тамбурное помещение перед переговорной, дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему 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 1В. В таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 2 - Устройства активной защиты

Модель	Цена, руб.	Характеристики	Особенности
Буран-2	81 000	Диапазон рабочих частот 180–11200 Гц	<ul style="list-style-type: none">• число помеховых каналов – три (виброакустических – 2, акустических – 1);• возможность подключения большого числа преобразователей - до 50 шт. (виброакустических – до 40 шт., акустических – до 10 шт.);• прецизионная система параллельного контроля линий подключения преобразователей;• вывод информации о состоянии работы системы на жидкокристаллический индикатор;• встроенная перестраиваемая система активной защиты информации от утечки по техническим каналам с программным управлением;• оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки;• возможность дистанционного включения системы по проводному каналу.
БАРОН	62 500	Диапазон рабочих частот 60–16000 Гц	<ul style="list-style-type: none">• Диск с ПО;• Кабель для записи сформированных помех в клонеры через последовательный порт ПЭВМ;• Модуль ДУ по радиоканалу (дополнительная опция);• Сетевой шнур;• Руководство по эксплуатации;• Техническая документация;
ЛГШ-404	23 580	Диапазон рабочих частот 90–11200 Гц	Устройство представляет собой генератор виброакустического шума, обеспечивающий генерацию "белого" шума с равномерной спектральной плотностью в заданном диапазоне частот с нормальным законом распределения плотности вероятности мгновенных значений. Изделие обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи.

По результатам анализа в качестве устройства активной защиты была выбрана модель “Барон”. Данная модель обладает наибольшим диапазоном рабочих частот, а также сравнительной дешевизной и качеством встроенных компонент.

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.

Устройства для перекрытия данных каналов утечки информации приведены в таблице 3.

Таблица 3 - Устройства активной защиты

Модель	Цена, руб.	Характеристики	Особенности
SEL SP-44	24 000	Устройство активной защиты информации от утечки по цепям электропитания и заземления (генератор регулируемого шума по электросети) SEL SP-44 предназначено для защиты информации, обрабатываемой техническими средствами и системами, путём формирования шумового сигнала маскирующих помех в цепях электропитания и заземления.	<ul style="list-style-type: none"> ● Цифровое автономное управление и контроль за настройками с защитой от несанкционированного доступа и выводом информации на встроенный жидкокристаллический экран. ● Применение двух некоррелируемых формирователей шума для цепей «фаза»-«земля» и «ноль»-«земля» позволяет исключить возможность съёма информационного сигнала как для противофазной, так и для синфазной схем подключения. ● Наличие независимых регуляторов уровня для низкочастотного и высокочастотного диапазонов позволяет оптимизировать спектр помехи по электромагнитной совместимости при сохранении достаточной эффективности маскировки. ● Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. ● Наличие встроенного счётчика суммарного времени наработки генератора помех с регистрацией значений в защищённой энергонезависимой памяти.
СОНАТА-ФС10.1	50 400	Предназначено для защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами,	Изделие представляет собой фильтр нижних частот, пропускающий сигнал на частоте напряжения линии электропитания и подавляющий высокочастотные сигналы и предназначено для подключения его к

		от утечки за счет побочных электромагнитных наводок информативного сигнала на линии электропитания напряжением 220 В с частотой 50 Гц.	однофазной линии электропитания 220 В, 50 Гц по 3-проводной схеме.
ЛГШ-221	36 400	Изделие предназначено для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок путем формирования маскирующих шумоподобных помех. Изделие является средством активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания, выходящие за пределы контролируемой зоны. Изделие соответствует 2 классу защиты и может устанавливаться в выделенных помещениях до 2 категории включительно.	<ul style="list-style-type: none"> • 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»).

По результатам анализа в качестве устройства активной защиты была выбрана модель “СОНАТА-ФС10.1”. Несмотря на цену, данное устройство обладает лучшими характеристиками и качеством компонентов на рынке, имеет множество положительных отзывов, и при относительно невысокой цене является лучшим выбором среди конкурентов.

5.3 Защита от ПЭМИН

Использование компьютеров и другой техники при обработке конфиденциальной информации создает побочные электромагнитные излучения. Они могут быть перехвачены и преобразованы в данные.

Снижение уровня сигнала и создание условий, исключающих возможность его перехвата, становятся основными принципами борьбы с угрозами утечки информации по каналам ПЭМИН.

Защита информации от утечки через ПЭМИН осуществляется с применением пассивных и активных методов и средств.

Пассивные методы защиты информации направлены на:

- ослабление побочных электромагнитных излучений (информационных сигналов) ОТСС на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

- ослабление наводок побочных электромагнитных излучений в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- исключение или ослабление просачивания информационных сигналов в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Активные методы защиты информации направлены на:

- создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала;
- создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала.

Средства активной защиты от утечки по каналам ПЭМИН:

- Тип «А» – Средства активной защиты информации от утечки за счет побочных электромагнитных излучений;
- Тип «Б» – Средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.

Оба средства предназначены для защиты информации категорий: совершенно секретно, секретно, особой важности и конфиденциальной информации.

Для построения системы защиты оптических каналов данного по варианту объекта были реализованы следующие мероприятия:

1. Выбрана элементная база технических средств компьютерной системы с возможно более малым уровнем информационных сигналов;
2. Произведена замена в информационных каналах компьютерной системы электрических цепей волоконно-оптическими линиями;

3. Выполнено локальное экранирование узлов технических средств, являющихся первичными источниками информационных сигналов;
4. Было включено в состав информационных каналов компьютерной системы устройство предварительного шифрования обрабатываемой информации;
5. В помещениях, где установлены средства обработки защищаемой информации, были использованы генераторов шума в целях зашумления (радиомаскировки).

Устройства для перекрытия данных каналов утечки информации приведены в таблице 4.

Таблица 4 - Устройства активной защиты

Модель	Цена, руб.	Характеристики	Особенности
Соната-РЗ	97 200	Соната-РЗ" - сертификат ФСТЭК России № 3514 от 05 февраля 2016 года удостоверяет, что средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок "Соната-РЗ", производимое в соответствии с техническими условиями ЮДИН.665820.014 ТУ является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа "А" и "Б", соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 1 классу защиты, может применяться в выделенных помещениях до 1 категории включительно.	<ul style="list-style-type: none"> комбинированный характер защиты (электромагнитное излучение + шумовое напряжение в линии электропитания и заземления); наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений; 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; встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией; возможность удаленного управления изделием как в случае автономного использования (непосредственно Пультом-ДУ4.2), так и в случае использования в составе комплекса ТСЗИ; наличие счетчика наработки в режиме «Излучение».
ЛГШ-503	44 200	Генераторы радиопомех предназначены для работы в составе систем активной защиты информации (САЗ), обеспечивая защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.	<ul style="list-style-type: none"> 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»)
Стикс-4	64 200	Система «Стикс-4» предназначена для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН) на объектах до 2-ой категории включительно.	<ul style="list-style-type: none"> предназначена для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок на объектах до 2-ой категории включительно система осуществляет защиту информации от утечки:

		<p>Система осуществляет защиту информации от утечек за счет:</p> <ul style="list-style-type: none"> • побочных электромагнитных излучений путем создания в диапазоне частот 0,01 - 1800 МГц электромагнитного поля маскирующего шума вокруг технических средств и подключенных к ним периферийных устройств, цепей электропитания и кабелей передачи данных; • за счет наведения шумового электрического сигнала в отходящие от СЗИ «Стикс-4» линии электропитания и заземления, а также в токопроводящие линии и инженерно-технические коммуникации в диапазоне частот 0,01 - 400 МГц. <p>Для излучения в эфир сформированного шумового сигнала используется антенна, установленная внутри корпуса устройства. Система защиты информации «Стикс-4» оснащена счетчиком наработки, индицирующим суммарное время работы СЗИ в часах в режиме генерации маскирующего шума. Максимальное индицируемое время 99 999 ч. Также присутствует визуальная индикация нормального режима работы и визуально-звуковая сигнализация отказа.</p>	<ul style="list-style-type: none"> ○ за счет побочных электромагнитных излучений путем создания в диапазоне частот 0,01 - 1800 МГц электромагнитного поля маскирующего шума вокруг технических средств и подключенных к ним периферийных устройств, цепей электропитания и кабелей передачи данных ○ за счет наведения шумового маскирующего электрического сигнала в отходящие от СЗИ «Стикс-4» линии электропитания и заземления, а также в токопроводящие линии и инженерно-технические коммуникации в диапазоне частот 0,01 - 400 МГц • равномерность огибающей спектра шумового сигнала в полосе до 1800 МГц с возможностью расширения полосы до 2500 МГц • высокая эффективность (соотношение излучаемой и потребляемой мощности) по сравнению с существующими аналогами • изделие выполнено в компактном форм-факторе блока питания со штепсельной вилкой и розеткой для подключения защищаемой вычислительной техники • система проста в установке и не требует проведения монтажных работ по установке внешних антенн • система обладает малым энергопотреблением, что позволяет, не создавая заметных нагрузок, запитывать ее от резервных источников питания • для наведения шумового сигнала на токопроводящие линии (за исключением линий электропитания) и инженерно-технические коммуникации необходимо использовать излучатель линейный (ИЛ) • система не создает акустического шума
--	--	---	---

По результатам анализа в качестве устройства активной защиты была выбрана модель “Соната-РЗ”. Несмотря на цену, данное устройство обладает лучшими характеристиками и качеством компонентов на рынке, имеет множество положительных отзывов, и при относительно невысокой цене является лучшим выбором среди конкурентов.

5.4 Защита от утечек по визуально-оптическому каналу

Основным способом борьбы с утечкой информации по оптическим каналам связи остается затруднение доступа злоумышленника к объектам, содержащим секретные данные. Вторая задача — выявление закладных устройств по следующим принципам:

- фиксация радиосигнала;
- фиксация повышенного электромагнитного излучения;
- просвечивание рентгеновскими лучами с целью выявления проводников;
- поиск проводов, ведущих неизвестно куда.

Для построения системы защиты оптических каналов данного по варианту объекта были реализованы следующие мероприятия:

1. Для защиты от утечки информации из выделенного помещения по оптическому каналу через окна были применены средства ослабления отраженного света: жалюзи, темные и рефлекторные стекла;
2. Использованы методы энергетического скрытия: уменьшена освещенность объектов защиты;
3. Применены методы структурного скрытия объектов защиты, в частности архивных шкафов, при помощи варьирования отражательных характеристик и контрастов между цветом и освещенностью фона и объекта.

6 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В соответствие с вышеуказанными устройствами, выбранными в качестве защиты информации на предприятии, составим смету (Таблица 5).

Таблица 5 - Смета

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
БАРОН (акустоизлучатель)	1 890	25	47 250
БАРОН (вибровозбудитель)	1 800	33	59 400
Соната-РЗ	97 200	1	97 200
СОНАТА-ФС10.1	50 400	6	302 400
Blackout-жалюзи	1600	3	4 800
Звукоизолирующая дверь "МТМ-ПРО"	24 000	4	96 000
ИТОГО			607 050

Размещение устройств представлено на рисунке 5.

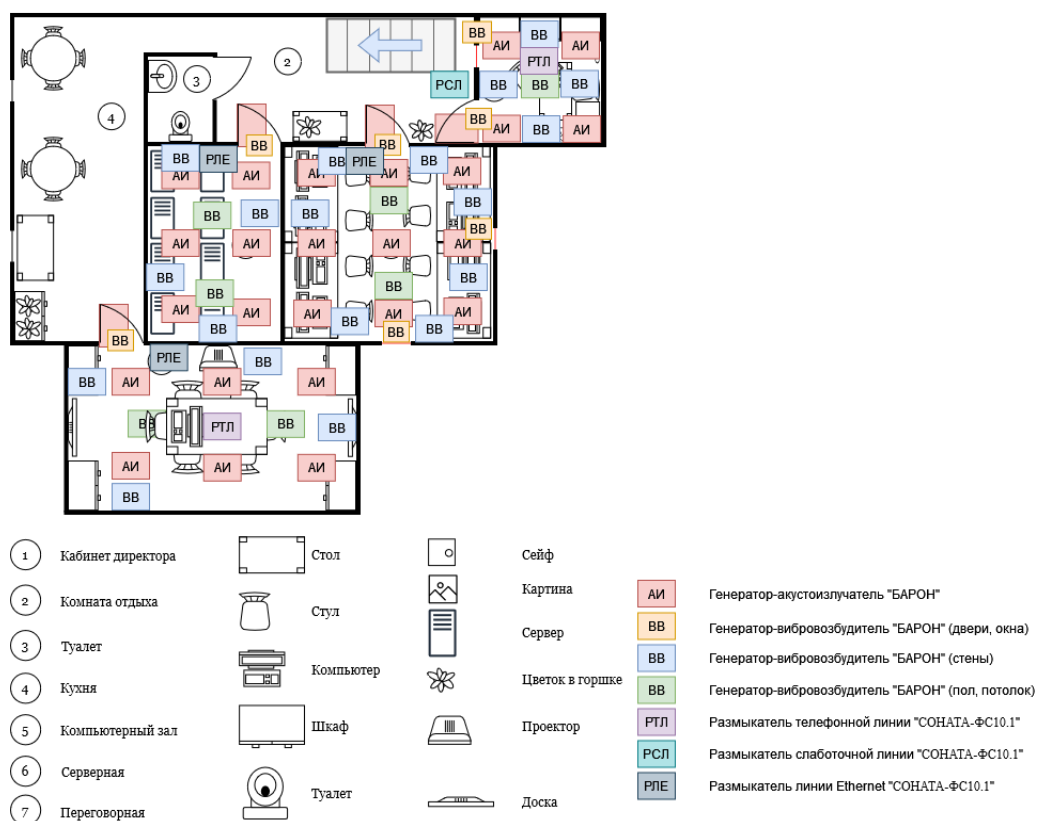


Рисунок 5 - Схема размещения устройств в офисе

ЗАКЛЮЧЕНИЕ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат.

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Способы предотвращения утечки информации | Способы и средства защиты информации от утечки по техническим каналам - SearchInform. Дата просмотра: 22.10.2022
searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/.
- 2 Каналы утечки информации на предприятии - SearchInform. Дата просмотра: 22.10.2022
searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/kanaly-utechki-informatsii-na-predpriyatii/.
- 3 Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам. Дата просмотра: 22.10.2022
learn.urfu.ru/resource/index/data/resource_id/40977/revision_id/0.