

**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 инженерно-технической системы защиты информации на предприятии.

Вариант 108»

**Выполнила:**

студент группы N34511

Вернигорова Анастасия Анатольевна

  
\_\_\_\_\_  
(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**

<b>Студент</b>	Вернигорова А.А. <div>(Фамилия И.О.)</div>
<b>Факультет</b>	факультет безопасности информационных технологий
<b>Группа</b>	N34511
<b>Направление (специальность)</b>	10.03.01 (Информационная безопасность)
<b>Руководитель</b>	Попов И.Ю. <div>(Фамилия И.О.)</div>
<b>Должность, ученое звание, степень</b>	доцент факультета БИТ, к.т.н.
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 108
<b>Задание</b>	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 планом помещений

**Содержание пояснительной записки**

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.

---

7. Заключение.

---

8. Список литературы.

---

**Рекомендуемая литература**

Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак Защита информации техническими средствами.

---

**Руководитель**

---

(Подпись, дата)

**Студент**



---

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

<b>Студент</b>	Вернигорова А.А. (Фамилия И.О)
<b>Факультет</b>	факультет безопасности информационных технологий
<b>Группа</b>	N34511
<b>Направление (специальность)</b>	10.03.01 (Информационная безопасность)
<b>Руководитель</b>	Попов И.Ю. (Фамилия И.О)
<b>Должность, ученое звание, степень</b>	Доцент факультета БИТ, к.т.н.
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 108

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023	01.10.2023	
2.	Анализ теоретической составляющей	10.10.2023	10.10.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.10.2023	20.10.2023	
4.	Представление выполненной курсовой работы	07.11.2023	07.11.2023	

**Руководитель** \_\_\_\_\_  
(Подпись, дата)

**Студент** \_\_\_\_\_  
(Подпись, дата)

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Вернигорова А.А. (Фамилия И.О)
<b>Факультет</b>	факультет безопасности информационных технологий
<b>Группа</b>	N34511
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации 2019)
<b>Руководитель</b>	10.03.01 (Информационная безопасность) Попов И.Ю. (Фамилия И.О)
<b>Должность, ученое звание, степень</b>	
<b>Дисциплина</b>	Доцент факультета БИТ, к.т.н.
<b>Наименование темы</b>	Инженерно-технические средства защиты информации Проектирование инженерно-технической системы

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

<b>1. Цель и задачи работы</b>	Целью работы является повышение уровня защищенности рассматриваемого помещения. Задачами являются проведение анализа защищаемого помещения с целью выявления возможных каналов утечки информации и выбор достаточных мер пассивной и активной защиты информации.
<b>2. Характер работы</b>	Конструирование
<b>3. Содержание работы</b>	1. Введение; 2. Анализ технических каналов утечки информации; 3. Руководящие документы; 4. Анализ защищаемых помещений; 5. Анализ рынка технических средств; 6. Описание расстановки технических средств;

---

7. Заключение;

---

8. Список литературы.

---

**4. Выводы**

---

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

---

**Руководитель**

---



(Подпись, дата)

**Студент**

---

(Подпись, дата)

## СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	7
ВВЕДЕНИЕ	8
1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ	10
1.1.1 Визуально-оптические каналы утечки информации	12
1.1.2 Акустические каналы утечки информации	13
1.1.3 Электромагнитные каналы утечки информации	14
1.1.4 Материально-вещественные каналы утечки информации	15
2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ	17
3 КРАТКАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИИ	20
4 ИНФОРМАЦИОННЫЕ ПОТОКИ	23
5 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	29
5.1 Описание помещений	29
5.2 Анализ возможных утечек информации	30
5.3 Выбор средств защиты информации	30
6 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	32
6.1 Защита информации от утечки по акустическими и виброакустическим каналам утечки информации	32
6.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	36
6.3 Защита от ПЭМИН	39
6.4 Защита от утечек по оптическому каналу	41
7 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	43

## **ВВЕДЕНИЕ**

В современном мире эффективное функционирование организации невозможно без стратегического управления информацией. Неотъемлемой частью этого процесса является обеспечение безопасности обрабатываемых данных. В связи с активным внедрением современных технологических решений в бизнес-процессы, защита конфиденциальной информации и активов организации приобретает особую значимость, поскольку повсеместно внедряемые новые технологические решения могут представлять собой серьезные угрозы безопасности активов предприятия.

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

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, к которой относятся информация ограниченного доступа, в частности сведения, составляющие коммерческую тайну, а также персональные данные лиц, являющихся и не являющихся работниками Оператора, а также иная информация, обрабатываемая на объекте информатизации. Защищаемый объект представляет собой этаж офисного здания, отведенный под центральный офис организации, включающий в себя следующие защищаемые помещения:

- переговорная;
- отдел взаимодействия с поставщиками;
- секретариат;
- дирекция;
- юридический отдел;
- отдел кадров;
- отдел бухгалтерского учета и отчетности (бухгалтерия);



- отдел продаж;
- проектный отдел;
- кабинет начальника службы информационной безопасности;
- служба информационной безопасности.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень руководящих документов. В третьей проведен анализ защищаемых помещений с точки зрения возможных каналов утечки информации и требуемых технических средств для обеспечения защиты обрабатываемой информации. Четвертая глава представляет собой анализ рынка технических средств защиты информации. Пятая глава посвящена разработке схемы расстановки выбранных технических средств на защищаемом объекте.

# **1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Утечкой информации считают бесконтрольный выход охраняемых сведений за пределы организации или круга лиц, которым они были доверены по службе или стали известны в процессе работы.

Причины утечки информации связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, рекламной, издательской, отчетной, информационной и иной деятельности предприятия (организации) и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут, например, относиться::

- 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;
- отсутствие эффективного мониторинга и контроля над средствами защиты информации;
- постоянная смена сотрудников, которые занимаются защитой конфиденциальной информации.

Таким образом, большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

Кроме того, утечке информации способствуют:

- стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение);
- неблагоприятная внешняя среда (гроза, дождь, снег);
- катастрофы (пожар, взрывы);
- неисправности, отказы, аварии технических средств и оборудования

По аналогии с каналом передачи информации канал, по которому осуществляется скрытая передача информации из одной точки в другую, независимо от желания объекта или

источника, называют каналом утечки информации. Он также состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышленника (Рисунок 1.1). Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику.



Рисунок 1.1 - Структура канала утечки информации

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.

В рамках данной курсовой работы рассматриваются исключительно технические каналы утечки информации (Рисунок 1.2).

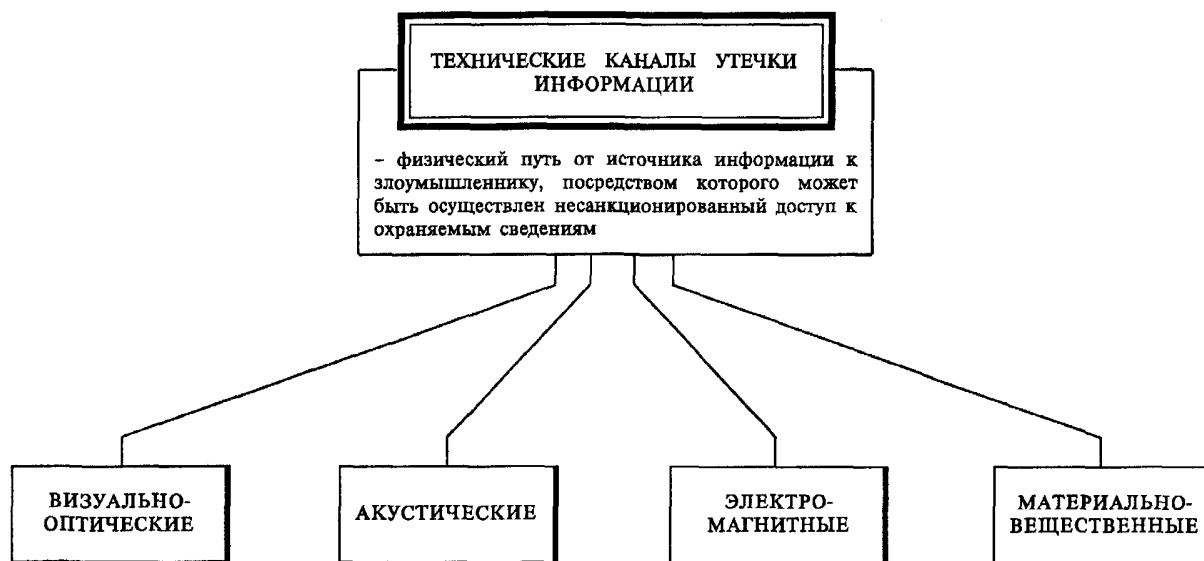


Рисунок 1.2 - Классификация технических каналов утечки информации

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.

### 1.1.1 Визуально-оптические каналы утечки информации

Визуально-оптические каналы - это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах.

В оптических технических каналах утечки информации производится перехват видовой информации с помощью оптических приборов.

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.

Другая классификация визуально-оптических каналов приведена на Рисунке 1.3.

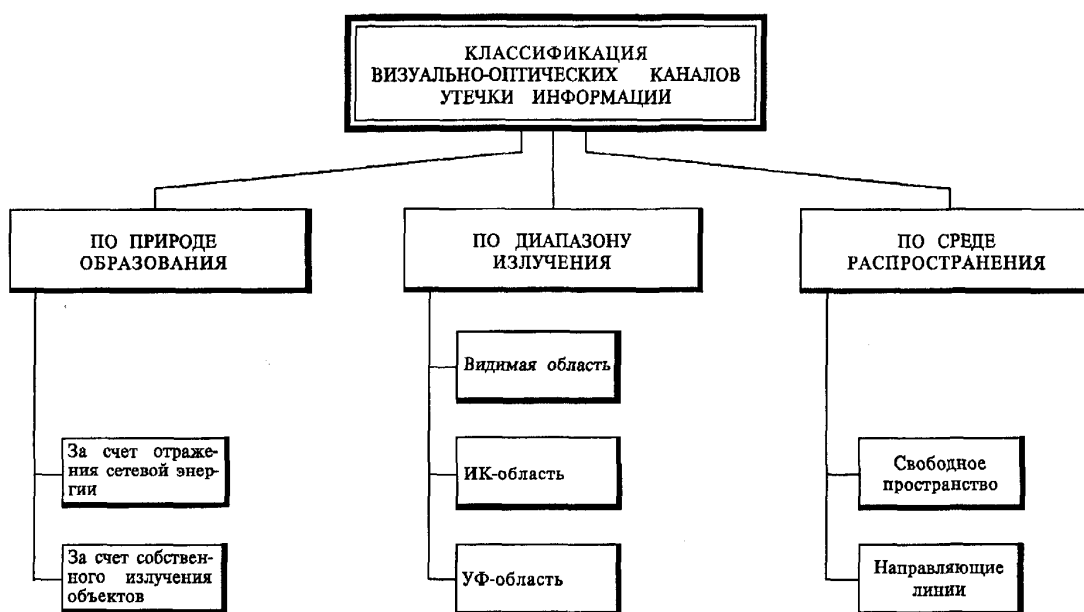


Рисунок 1.3 - Классификация визуально-оптических каналов утечки информации

### 1.1.2 Акустические каналы утечки информации

Акустическими называют технические каналы утечки информации, которые образуются при прохождении звуковых волн через воздух, жидкие или твердые материалы.

Выделяют следующие разновидности акустического канала утечки информации:

- Прямой акустический (воздушный) (перехват речевой информации производится с помощью чувствительных направленных микрофонов);
- Виброакустический (злоумышленники используют устройства для улавливания вибрационных колебаний, вызываемых давлением звуковых волн на строительные конструкции зданий);
- Электроакустический (акустоэлектрический) (утечка информации происходит из-за преобразования звукового сигнала в электрический при прохождении акустических волн через ВТСС);
- Оптико-акустический (акустооптический) (причиной потери данных является «микрофонный» эффект);
- Параметрический (поле, создаваемое источником акустического сигнала, может изменять параметры электромагнитных устройств, используемых злоумышленниками).

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.

### 1.1.3 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.

Классификация электромагнитных каналов утечки информации приведена на Рисунке 1.3.

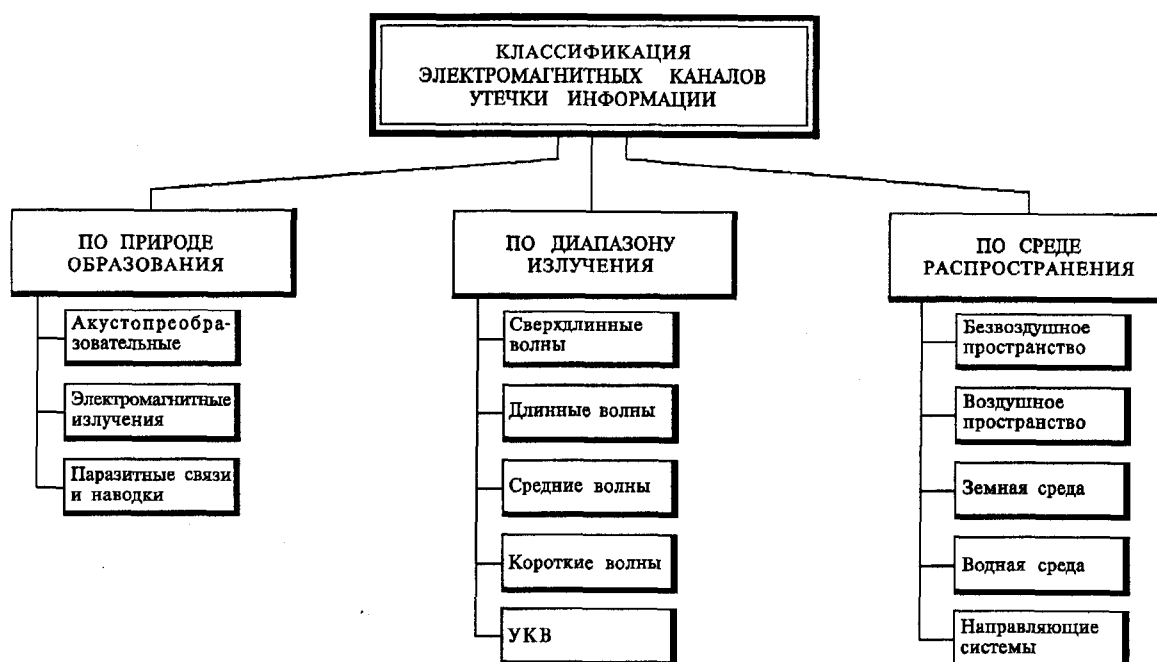


Рисунок 1.4 – Классификация электромагнитных каналов утечки информации

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.

Перехват информации возможен путём «высокочастотного облучения» («электромагнитного навязывания») ТСПИ. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение имеет модуляцию, обусловленную воздействием информационного сигнала.

Поскольку переизлученное электромагнитное поле имеет параметры, отличные от облучающего поля, данный канал утечки информации часто называют параметрическим.

Для перехвата информации по параметрическому каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные приёмные устройства.

#### **1.1.4 Материально-вещественные каналы утечки информации**

В материально-вещественных технических каналах утечки информации источниками информации становятся материальные объекты, выносимые за пределы рабочей зоны.

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое. Материально-вещественные технические каналы утечки информации классифицируют, учитывая физическое состояние информационных объектов, природу объектов перехвата, виды носителей. Классификация материально-вещественных каналов утечки информации представлена на Рисунке 1.5.

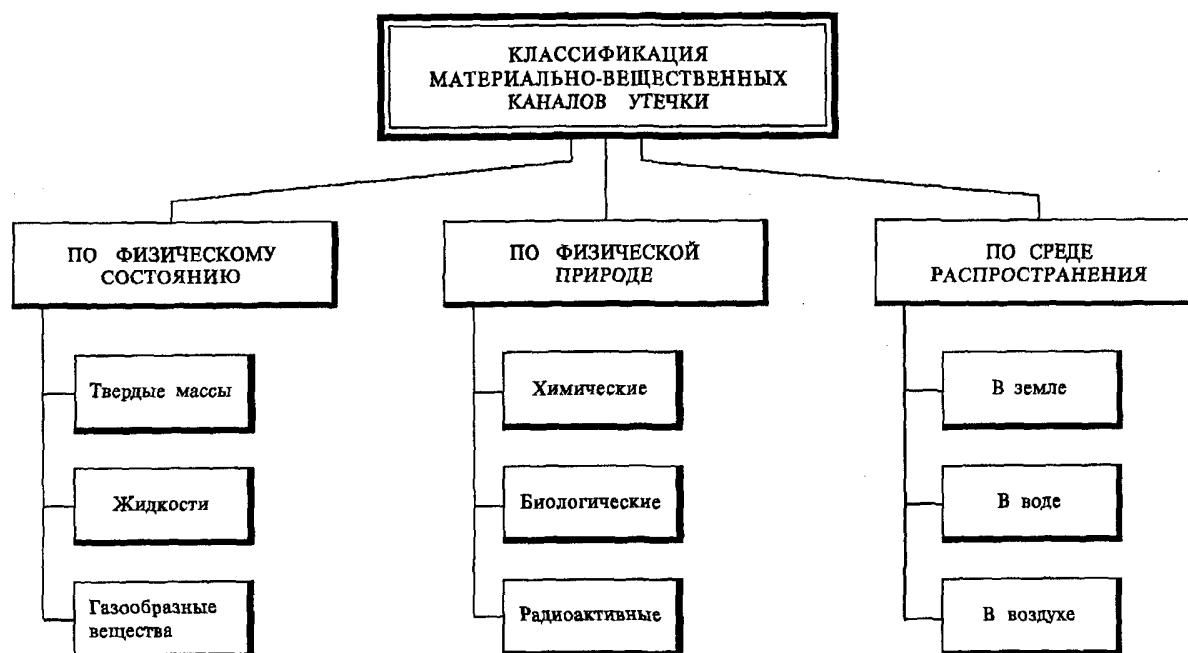


Рисунок 1.5 – Классификация материально-вещественных каналов утечки информации



## **2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ**

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ ФСБ России от 10.07.2014 г. № 378 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Федеральный закон от 28.12.2010 N 390-ФЗ «О безопасности»;
- Постановление Правительства РФ от 22.11.2012 N 1205 «Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны»;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. От 21.04.2010) «О сертификации средств защиты информации»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;
- Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними"
- Федеральный закон от 29.07.2004 г. N 98-ФЗ "О коммерческой тайне";
- Указ Президента РФ от 06.03.1997 г. N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 02.06.2020 г. № 76 "Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к технической

защиты информации и средствам обеспечения безопасности информационных технологий";

- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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 Концепция защиты средств вычислительной техники и автоматизированных систем 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 КРАТКАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИИ

Наименование организации: общество с ограниченной ответственностью “InEsthetic” (далее - ООО "InEsthetic", Общество).

Область деятельности: студия дизайна интерьера.

Организация ООО "InEsthetic" предназначена для выполнения функций, связанных с разработкой дизайна интерьера и созданием уникальных, эстетичных и функциональных интерьерных решений. Главные задачи и функции компании включают в себя:

1. Консультирование и разработка дизайн-проектов: компания предоставляет клиентам профессиональные консультации по оформлению интерьера и разрабатывает дизайн-проекты и индивидуальные интерьерные решения, учитывающие желания и потребности заказчиков.
2. Подбор стиля и материалов: компания помогает клиентам выбрать оптимальный стиль дизайна, цветовую палитру и материалы, которые соответствуют их вкусу и бюджету.
3. Создание эскизов и визуализации: компания разрабатывает эскизы и визуализации проекта, позволяя клиентам визуально представить, как будет выглядеть их интерьер после реализации дизайн-концепции.
4. Поставка и установка мебели и декора: компания предоставляет услуги по подбору, доставке и установке мебели, аксессуаров и декоративных элементов, необходимых для завершения интерьера.

Таким образом, Общество специализируется на предоставлении полного спектра услуг в области дизайна интерьера, с целью создания привлекательных, комфортабельных и функциональных жилых и коммерческих пространств.

Основные и функциональные бизнес-процессы, а также реализованные в рамках них бизнес-функции Общества представлены в Таблице 2.1.

Таблица 2.1 – Бизнес-процессы и бизнес-функции Общества

Наименование бизнес-процесса	Наименование бизнес-функции
Разработка дизайн-проектов	Подбор стиля и материалов
	Создание эскизов и визуализации

	Разработки индивидуальных интерьерных решений
	Выбор мебели и декора
Работа с клиентами	Консультирование
	Коммуникация в рамках работы над проектом
Маркетинг	Определение целевой аудитории
	Исследование рынка
	Разработка маркетинговой стратегии
	Разработка рекламной кампании и продвижение товара на рынке
Закупки и управление поставками	Планирование закупок
	Согласование цен и условий поставки
	Заключение контрактов
	Контроль качества поставляемой продукции
	Управление отношениями с поставщиками
Управление складом	Контроль за поступлением товара на склад
	Учет и хранение товара
	Комплектация заказов
	Отгрузка товара со склада
Бухгалтерский и налоговый учет	Ведение документации
	Анализ финансовых показателей
Безопасность и сохранность активов	Обеспечение физической безопасности
	Обеспечение информационной безопасности
Соответствие законодательству	Обеспечение соответствия требованиям законодательства
	Взаимодействие с контрольными (надзорными) органами
Управление персоналом	Найм персонала
	Обучение персонала
	Управление работой персонала
Стратегическое развитие	Анализ внешней и внутренней среды организации
	Выработка стратегии развития
	Мониторинг и контроль за реализацией стратегических целей

ИТ-системы и средства связи	Установка ПО
	Управление сетевым оборудованием
	Поддержка и обновление систем и ПО
	Администрирование баз данных

Схематичная структура Общества представлена на Рисунке 3.1.

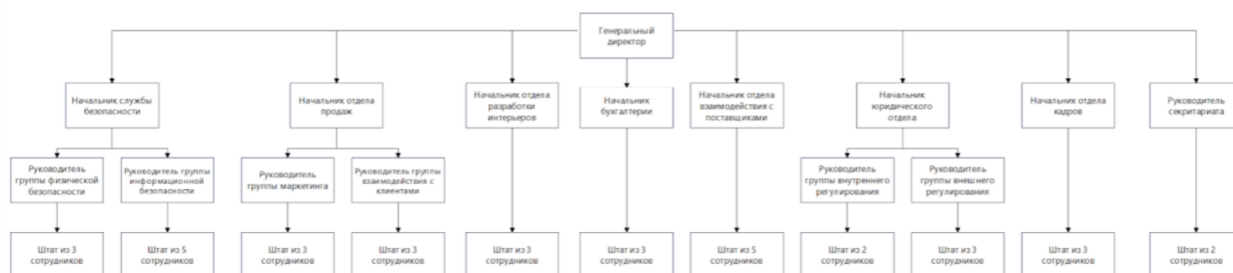


Рисунок 3.1 - Структура организации ООО “InEsthetic”

## 4 ИНФОРМАЦИОННЫЕ ПОТОКИ

В организации обрабатывается информация конфиденциального характера:

- персональные данные лиц являющихся и не являющихся работниками Общества;
- 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 особые 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 Общества представлены на Рисунках 4.1 и 4.2.

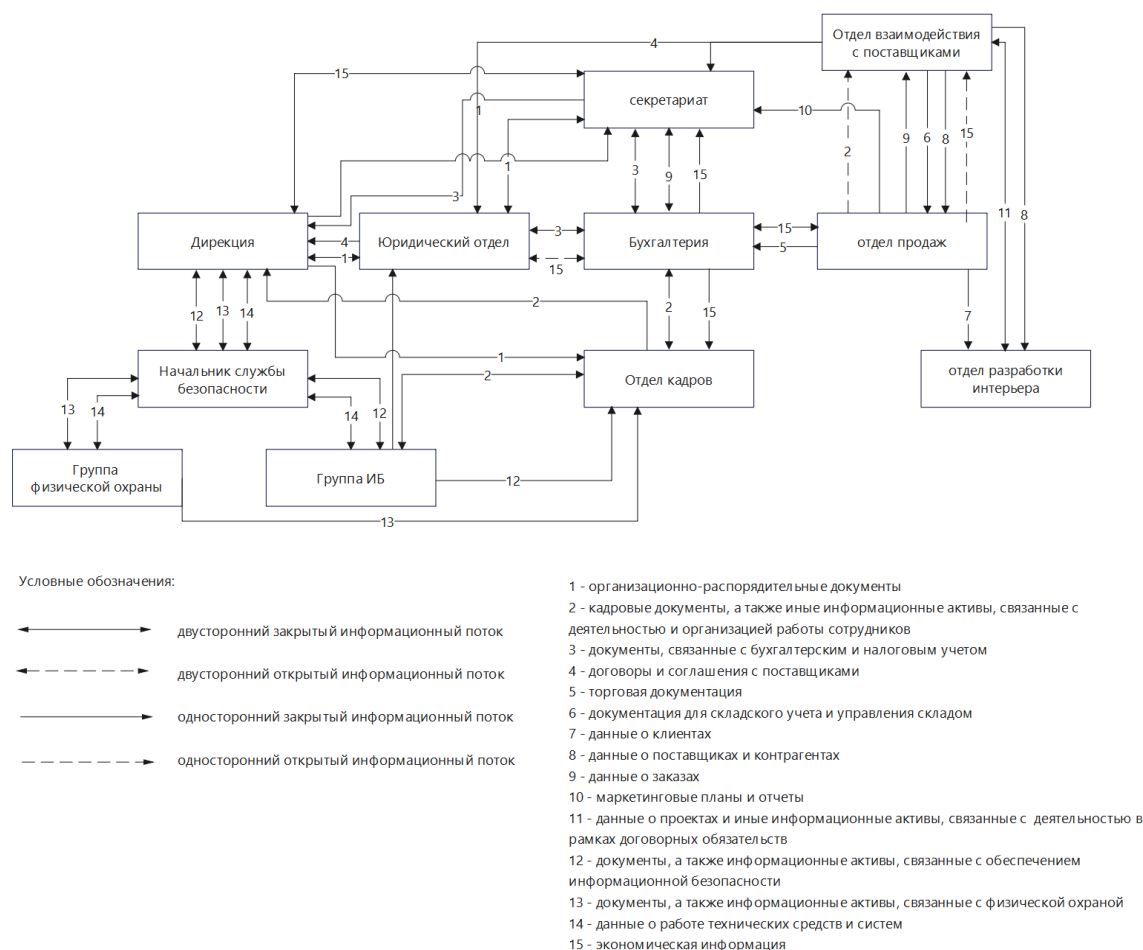


Рисунок 4.1 - Внутренние информационные потоки организации ООО “InEsthetic”

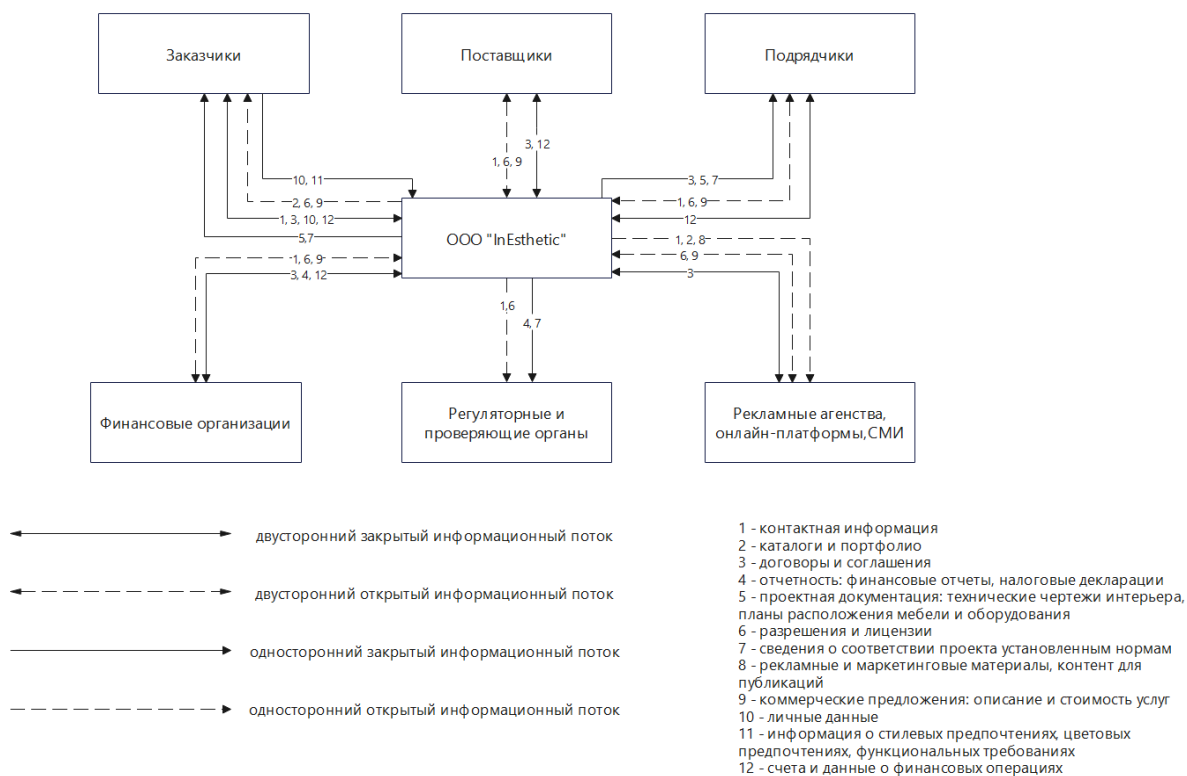


Рисунок 4.2 - Внешние информационные потоки организации ООО “InEsthetic”



Перечень информационных активов ООО “InEsthetic” представлен в Таблице 4.1  
Таблица 4.1 – Перечень информационных активов Общества

№ п/п	Наименование	Подтип	Функциональное назначение
1	Учредительные документы	Каталог с файлами, печатные документы	Содержат информацию о структуре, правовом статусе и участниках компании. Используются для установления правовых основ деятельности
2	Кадровые документы	Каталог с файлами, печатные документы	Регулирование процесса управления персоналом
3	Документы, связанные с бухгалтерским и налоговым учетом	Каталог с файлами, печатные документы	Обеспечение ведения бухгалтерского и налогового учета, соблюдение законодательных требований и норм
4	Договоры и соглашения с поставщиками	Каталог с файлами, печатные документы	Регулирование взаимоотношений с поставщиками товаров
5	Торговая документация	Каталог с файлами, печатные документы	Документирование процесса продажи товаров и услуг, оформление заказов, заключение договоров
6	Эскизы и визуализации проектов и разработок	Каталог с файлами, печатные документы	Визуально представление идей и разработок для дальнейшего коммерческого использования в рамках проектов
7	Проектная документация	Каталог с файлами, печатные документы	Содержит детальное описание технических характеристик и требований к проектируемому интерьеру. В ней указываются особенности строительных работ, материалы, используемые в проекте, и спецификации для мебели и оборудования
8	Документация для складского учета	Каталог с файлами, печатные документы	Отражение движения товаров по проектам на складе, фиксация поступлений и отгрузок, контроль за остатками товаров, обеспечение актуальности информации для планирования поставок и управления запасам
9	График поставок	Файл	Определение сроков и объемов поставок, установление графика и регламента поставок, контроль за соблюдением графика, обеспечение непрерывности поставок товаров
10	Документация, используемая	Каталог с файлами, печатные документы	Фиксация информации о состоянии и качестве товара при его поставке на склад, обеспечение

	для фиксации результатов проверки товара при его поставке на склад		контроля за соответствием товара заявленным характеристикам
11	Данные о клиентах	База данных	Обеспечение учета клиентской базы, анализ предпочтений и потребностей клиентов, планирование маркетинговых акций, улучшение обслуживания клиентов, повышение лояльности
12	Схема базы данных о клиентах	Схема базы данных	Описание структуры и взаимосвязи данных, хранящихся в базе данных о клиентах
13	Данные о поставщиках и контрагентах	База данных	Учет и обработка информации о поставщиках и контрагентах, контроль за исполнением договорных обязательств, планирование и управление взаимоотношениями с партнерами
14	Схема базы данных о поставщиках и контрагентах	Схема базы данных	Описание структуры и взаимосвязи данных, хранящихся в базе данных о поставщиках и контрагентах
15	Данные о заказах	База данных	Учет заказов, обработка заказов, контроль за выполнением и отгрузкой товаров, своевременное выполнение заказов, уведомление клиентов о статусе заказа
16	Схема базы данных о заказах	Схема базы данных	Описание структуры и взаимосвязи данных, хранящихся в базе данных о заказах
17	Данные о товарах	База данных	Учет и управление товарами, контроль за наличием и движением товаров, планирование закупок, обеспечение актуальности информации о товарах
18	Схема базы данных о товарах	Схема базы данных	Описание структуры и взаимосвязи данных, хранящихся в базе данных о товарах
19	Каталог товаров	Файл, печатный документ	Предоставление клиентам информации для выбора и покупки товаров, обеспечение удобства и наглядности представления ассортимента
20	Маркетинговые планы	Каталог с файлами	Планирование маркетинговых активностей, определение рыночной стратегии, привлечение и удержание клиентов, увеличение продаж и расширение рыночной доли
21	Маркетинговые отчеты	Каталог с файлами	Сбор, обработка и анализ данных о маркетинговых активностях, оценка эффективности, корректировка стратегии маркетинга

22	Стратегический план развития компании	Файл	Определение стратегических приоритетов, планирование развития и роста, установление основных принципов и стратегических решений
23	Отчеты о выполнении стратегического плана	Каталог с файлами	Анализ выполнения стратегического плана, оценка эффективности мероприятий
24	Записи камер видеонаблюдения	Каталог с файлами	Отслеживание и фиксация событий
25	Конфигурационные файлы системы видеонаблюдения	Конфигурационная информация	Определение параметров работы системы видеонаблюдения
26	Данные системы контроля и управления доступом	База данных	Хранение информации о правах доступа сотрудников и посетителей, контроль и регулирование доступа к ограниченным зонам и ресурсам
27	Конфигурационные файлы системы контроля и управления доступом	Конфигурационная информация	Определение параметров работы системы контроля и управления доступом
28	Аудитные логи (журналы аудита)	Каталог с файлами	Фиксация и хранение информации о событиях, связанных с безопасностью и использованием информационных ресурсов
29	Документы, связанные с обеспечением информационной безопасности	Каталог с файлами, печатные документы	Регламентация политик и процедур информационной безопасности, документирование требований и мер безопасности, управление рисками и защитой информации
30	Документы, связанные с пожарной безопасностью	Каталог с файлами, печатные документы	Регламентация требований и мер по пожарной безопасности, документирование процедур эвакуации, планов аварийного реагирования и обеспечения безопасности при возникновении пожара
31	Защищенные резервные копии данных	Каталог с файлами	Обеспечение безопасности и сохранности данных, возможность восстановления после сбоев
32	Протоколы проверок и акты, составленные	Каталог с файлами, печатные документы	Документирование результатов проверок со стороны контрольных органов

	контрольными органами		
33	Графики работы сотрудников	Каталог с файлами	Организация работы персонала
34	План обучения персонала	Файл	Обеспечение получения необходимых навыков и повышения квалификации персонала
35	Обучающие материалы	Каталог с файлами	Обучение и ознакомление сотрудников с установленными правилами и процедурами, обеспечение соответствия требованиям и стандартам работы
36	Документы, связанные с отчетностью о проведении обучения персонала	Каталог с файлами, печатные документы	Отслеживание и отчетность о проведенных обучающих мероприятиях, оценка и улучшение эффективности обучения
37	Лицензионные ключи активации ПО	Каталог с файлами	Активация и управление лицензионным ПО, обеспечение соответствия правовым требованиям и защита от нелегального использования
38	Документация по установке, настройке и обновлению систем и ПО	Каталог с файлами	Обеспечение корректности установки, настройки и обновления систем и ПО, обеспечение правильной и эффективной работы систем
39	Журналы установки и обновлений систем и ПО	Каталог с файлами	Фиксация информации о проведенных установках и обновлениях систем и программного обеспечения, регистрация изменений и контроль версий
40	Конфигурационные файлы ПО	Конфигурационная информация	Определение и хранение настроек ПО
41	Конфигурационные файлы сетевого оборудования	Конфигурационная информация	Определение и хранение настроек сетевого оборудования
42	Документация по настройке и обслуживанию сетевого оборудования	Каталог с файлами	Обеспечение корректности установки, настройки и обслуживания сетевого оборудования, обеспечение правильной и эффективной работы сети
43	Конфигурационные файлы баз данных	Конфигурационная информация	Хранение и определение настроек баз данных, определение структуры, прав доступа и других параметров баз данных

44	Сведения, составляющие гос. тайну	Каталог с файлами	Любая информация с установленным грифом "секретно"
----	-----------------------------------	-------------------	--

## 5 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

План центрального офиса Общества представлен на Рисунке 5.1, который детально отображает структуру и организацию физического пространства центрального офиса.

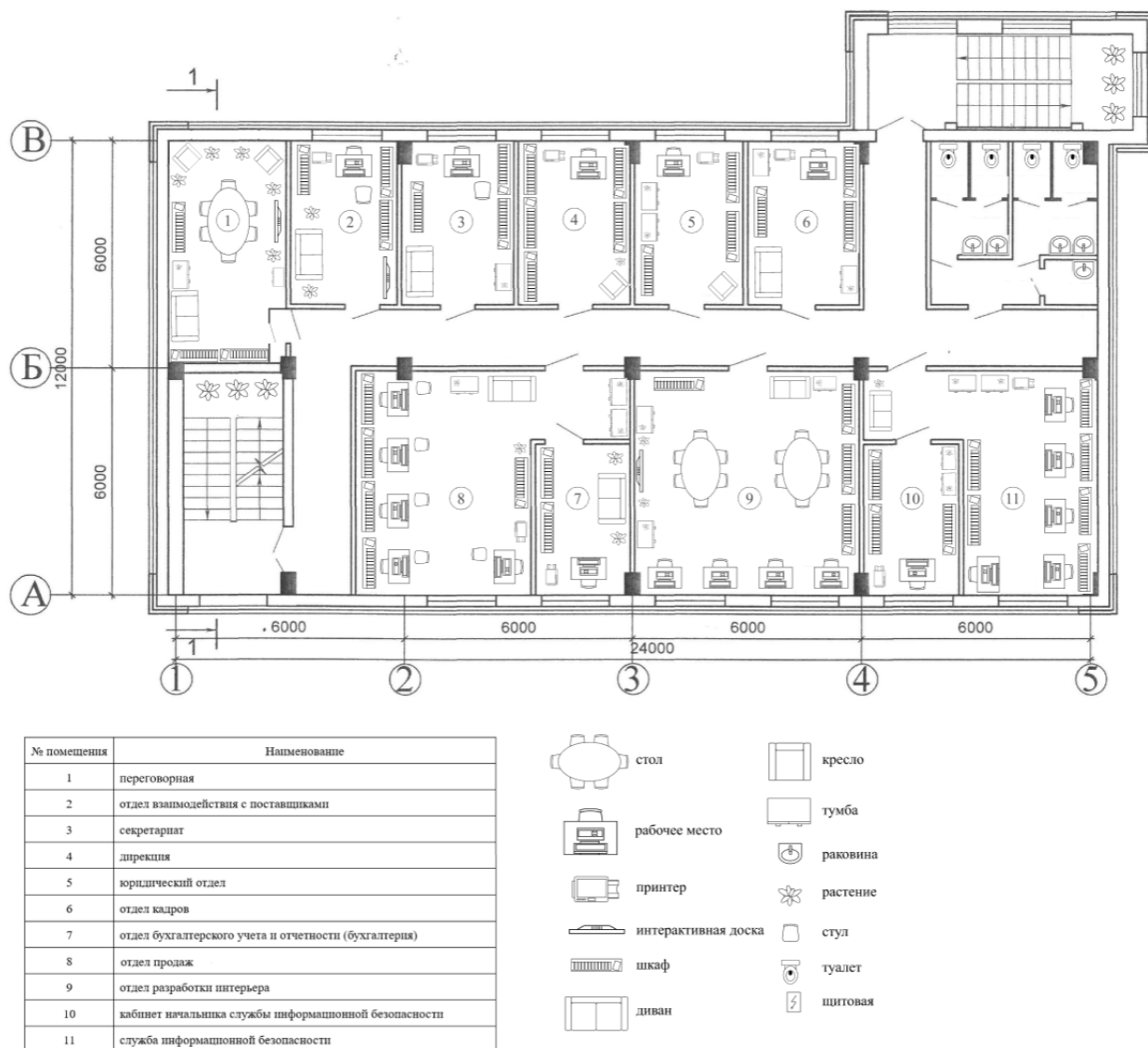


Рисунок 5.1 – План защищаемого помещения

### 5.1 Описание помещений

Защите подлежат следующие помещения:

- переговорная  $18\text{м}^2$  (6м x 3м);
- отдел взаимодействия с поставщиками  $15\text{м}^2$  (5м x 3м);
- секретариат  $15\text{м}^2$  (5м x 3м);
- дирекция  $15\text{м}^2$  (5м x 3м);

- юридический отдел  $15\text{м}^2$  (5м х 3м);
- отдел кадров  $15\text{м}^2$  (5м х 3м);
- отдел продаж  $32\text{м}^2$  (6м х 7м - 2.5м х 4м);
- отдел бухгалтерского учета и отчетности (бухгалтерия)  $10\text{м}^2$  (2.5м х 4м);
- проектный отдел  $36\text{м}^2$  (6м х 6м);
- кабинет начальника службы информационной безопасности  $10\text{м}^2$  (2.5м х 4м);
- служба информационной безопасности  $26\text{м}^2$  (6м х 6м - 2.5м х 4м).

Защищаемый объект расположен на третьем этаже пятиэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с наружными пожарными 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.

## **5.2 Анализ возможных утечек 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.

## **5.3 Выбор средств защиты информации**

В нашем случае подходит вторая категория объекта защиты: скрывание параметров информационных сигналов при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрывание информации, обрабатываемой на объекте)

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» – требуется оснастить помещение средствами защиты всех потенциальных технических каналов утечки информации,

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, в частности несущие стены и перегородки, перекрытия, коробки дверных проемов, стекла, трубы тепло- и водоснабжения, каналы вентиляции, батареи	Дополнительное помещение перед переговорной, изолирующие звук и вибрацию обшивки стен	Устройства вибрационного зашумления
Визуально-оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного зашумления



## **6 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

### **6.1 Защита информации от утечки по визуально-оптическому каналу утечки информации**

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

- располагать объекты защиты так, чтобы исключить отражение света в сторону возможного расположения злоумышленника;
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты;
- 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;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отраженного 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.

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

- для защиты от утечки информации по оптическому каналу через окна были применены средства ослабления отраженного света: жалюзи, темные и рефлекторные стекла;
- использованы методы энергетического сокрытия: уменьшена освещенность объектов защиты;
- применены методы структурного сокрытия объектов защиты, в частности архивных шкафов, при помощи варьирования отражательных характеристик и контрастов между цветом и освещенностью фона и объекта.

## **6.2 Защита информации от утечки по акустическими, электроакустическим и виброакустическим каналам утечки информации**

Основная идея пассивных средств защиты акустической информации - это снижение соотношения сигнал/шум в возможных точках перехвата информации за счет снижения информативного сигнала.

При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

- в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;
- в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;
- потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;
- в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками.

Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам.

Для снижения риска утечки информации по виброакустическому каналу специалистам по безопасности требуется максимально ослабить акустический сигнал от источника звука, подающийся на коммуникации, служащие средой его распространения, где он может быть перехвачен. Первым решением станет архитектурно-конструкторское: звуковую волну нужно вынудить пройти сначала среду с высоким затуханием, пористую или специально подготовленную с целью добиться максимальной звукоизоляции – например, с наполнением ватой, покрытием стен пористой штукатуркой.

Пассивная защита представляет собой усиленные двери с двойными коробками, тамбурное помещение перед переговорной, дополнительную отделку переговорной звукоизолирующими материалами. Внутренние двери однопольные, входные двери в стальные или деревянные (из столярной плиты) обитые железом.

Переговорная размещена на достаточно высоком этаже и не имеет окон.

В качестве перекрытий использованы акустически неоднородные конструкции с упругими прокладками (пробка, ДВП), что позволяет увеличить коэффициент звукоизоляции защищаемого помещения.

Потолки подвесные со звукоизолирующим слоем.

Вентиляционные каналы оборудованы специальными крышками из , позволяющими закрывать отверстие вентиляционного канала при ведении переговоров и открывать его, когда переговоры не ведутся.

Защита от утечек по виброакустическим каналам строится по трем стандартным принципам:

- предотвращение путем максимального снижения уровня сигнала;
- выявление;
- блокировка и зашумление сигнала, снижающие риск расшифровки.

Поглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными. Один из распространенных видов пористых материалов — облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит или рельефных конструкций (пирамид, клиньев и т.д.), располагаемых или вплотную, или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.).

Повышение звукоизоляции стен и перегородок помещений достигается применением слоистых или отдельных их конструкций. В многослойных перегородках и стенах целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон—поролон).

Звукоизолирующая способность сложных стен, имеющих дверные и оконные проемы, зависит от звукоизоляции дверей и окон. Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна дверей к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д. При недостаточной звукоизоляции однослойных дверей используются двойные двери с тамбуром, облицованные звукопоглощающим материалом.

Звукопоглощающая способность окон, так же как и дверей, зависит главным образом от поверхностной плотности стекла и прижатия притворов. Обычные окна с двойными переплетами обладают более высокой (на 4—5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях, когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной

конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20—40 мм и с воздушным зазором между стеклами не менее 100 мм). Повышенное звукопоглощение обеспечивается применением конструкции окон на основе стеклопакетов с герметизацией и заполнением зазора между стеклами различными газовыми составами.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, прокладок, глушителей, вязкоупругих заполнителей и т.д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием сложных акустических фильтров и глушителей.

Для активной защиты требуется сгенерировать в среде распространения сильный помеховый сигнал, который невозможно доступными злоумышленнику техническими средствами отфильтровать от информационного. Естественные помехи, связанные с работой систем ЖКХ, снижают уровень разборчивости сигнала, но к ним необходимо присоединить имеющие техническое происхождение. Для зашумления виброакустического канала утечки используют генераторы белого шума (электромагнитных помех), связанные с излучателями, устанавливаемые на стенах, стеклах, трубах отопления.

Рынок предлагает несколько моделей генераторов помех, наиболее мощные модели генераторов имеют сертификацию ФСТЭК. Вибровозбудители исключают возможность снятия полноценного акустического сигнала с различных типов проводников — стекол, жалюзи, труб. Некоторые модели могут быть установлены в запотолочном пространстве и между обычным и подвесным потолком, дверных тамбурах, системах вентиляции.

При помощи специальных переходников они крепятся к капитальным стенам (перекрытиям) из бетона, кирпича, трубам отопления, газовым трубам, защитной оболочке кабелей различного назначения и длительное время работают в автономном режиме. Также часто используются вибрационные преобразователи. Комбинированное средство виброакустической защиты сертифицировано ФСТЭК и может применяться для защиты от утечек по акустическому и виброакустическому каналу помещений, в которых обрабатываются данные, содержащие государственную тайну. Система формирует широкополосные акустические и вибрационные маскирующие шумовые помехи в воздушной среде, элементах ограждающих конструкций и в инженерно-технических

коммуникациях защищаемых помещений. Приборы управляются при помощи дистанционного пульта.

Генерация шума имеет следующие особенности:

- вместе с белым шумом создается речеподобный, что улучшает маскирующие характеристики, отделение потоков друг от друга становится маловероятным;
- мощность шума автоматически повышается при усилении речи, что улучшает степень защиты;
- маскирующие шумы не мешают рабочему процессу.

К прибору могут подключаться акустические, керамические, электромагнитные и пьезоизлучатели любого производителя.

Оптимальное количество акустоизлучателей и вибровозбудителей для каждого помещения определяется такими факторами, как его звукоизолирующие свойства, конфигурация, материалы ограждающих поверхностей, расположение помещения, уровень шумового фона и т.п.

Предварительная оценка необходимого количества вибровозбудителей "СВ-4Б1" может быть выполнена исходя 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 м<sup>2</sup> перекрытия;
- окна - один на окно (при установке на оконный переплет);
- двери - один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Ориентировочное количество акустоизлучателей "СА-4Б" может быть определено исходя из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м<sup>3</sup> надпотолочного пространства или др. пустот.

Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. В таблице 6.1 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 6.1 - Устройства активной защиты

Модель	Минимальная цена, руб.	Диапазон рабочих частот, Гц	Сертификат	Состав системы	Особенности
Соната-АВ модель 4Б	56160	175 - 11 200	Сертификат ФСТЭК России № 3625 от 20 сентября 2016 года (до 20 сентября 2024 года)	<ul style="list-style-type: none"> <li>- блок электропитания и управления "Соната-ИП4.1" (26400);</li> <li>- блок электропитания и управления "Соната-ИП4.2" (36000);</li> <li>- блок электропитания и управления "Соната-ИП4.3" (21600);</li> <li>- генератор-вибровозбудитель "СВ-4Б" (7440);</li> <li>- генератор-акустоизлучатель "СА-4Б" (7440);</li> <li>- размыкатель телефонной линии "Соната-ВК4.1" (6000);</li> <li>- размыкатель слаботочной линии "Соната-ВК4.2" (6000);</li> <li>- размыкатель линии Ethernet "Соната-ВК4.3" (6000);</li> <li>- пульт управления "Соната-ДУ4.3", опция (7680);</li> <li>- блок сопряжения с внешними устройствами "Соната-СК4.1", опция (18000);</li> <li>- блок сопряжения с внешними устройствами "Соната-СК4.2", опция (13440);</li> <li>- техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу "Соната-АВ4Л", в составе: генераторный блок "АВ-4Л" и вибровозбудитель "СП-4Л" (10320)</li> </ul>	<ul style="list-style-type: none"> <li>- возможность подключения к одному питающему шлейфу;</li> <li>- индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы;</li> <li>- потенциально более высокая стойкость защиты речевой информации вследствие статистической независимости возбуждения маскирующего шума во всех точках;</li> <li>- возможность построения системы автоматического контроля всех элементов Изделия "Соната-АВ" модель 4Б при минимально возможной стоимости оборудования и монтажа;</li> <li>- снижение затрат на создание единого комплекса ТСЗИ, т.к. единая линия связи и электропитания для генераторов-излучателей одновременно может использоваться в этом же качестве для других элементов комплекса</li> </ul>
ЛГШ-404	71600	175 - 11200	Сертификат ФСТЭК России № 3599 от 22 июля 2016 года (до 22 июля 2024 года)	<ul style="list-style-type: none"> <li>- генераторный блок "ЛГШ-404" (35100);</li> <li>- вибровозбудитель "ЛВП-10" (5200);</li> <li>- акустический излучатель "ЛВП-2А" (3700);</li> <li>- размыкатель слаботочных линий "ЛУР-2" (5600);</li> <li>- размыкатель телефонных линий "ЛУР-4" (5600);</li> <li>- размыкатель для Ethernet "ЛУР-8" (5600);</li> <li>- вибрэкран "ЛИСТ-1" (16400)</li> </ul>	<ul style="list-style-type: none"> <li>- конструкция изделия обеспечивает защиту органов регулировки выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним;</li> <li>- визуальная система индикации нормального режима работы и визуально-звуковая система индикации аварийного режима (отказа);</li> </ul>
Буран	84500	100 - 11200	Сертификат ФСТЭК России № 3657 от 09 ноября 2016 года (до 09 ноября 2024 года)	<ul style="list-style-type: none"> <li>- виброакустический генератор «Буран» (60000);</li> <li>- виброакустический генератор «Буран» с возможностью дистанционной автоматической настройки (80000);</li> <li>- вибропреобразователь для стен «Молот» с креплением (4300);</li> </ul>	<ul style="list-style-type: none"> <li>- высокое качество шумовой помехи за счет использования аналогового задающего генератора на базе шумодиода;</li> <li>- частотная коррекция спектра помехового сигнала каждого канала;</li> </ul>

				<ul style="list-style-type: none"> <li>- вибропреобразователь для коммуникаций «Серп-Т» с креплением (4300);</li> <li>- вибропреобразователь для рам «Серп-Р» с креплением (4300);</li> <li>- вибропреобразователь для окон «Копейка» (пьезоэлектрический) (3500);</li> <li>- вибропреобразователь для окон «Копейка-М» (электродинамический) (4300);</li> <li>- быстросъемное крепление на раму окна (для виброизлучателей "Копейка", "Копейка-М") (500)</li> <li>- вибропреобразователь для зашумляемого экрана «Копейка-ЛМ» (электродинамический) (4300);</li> <li>- преобразователь акустический «Рупор» (4300);</li> <li>- размыкатель аналоговых телефонных линий "Буран-К1" (5800);</li> <li>- размыкатель линий оповещения и сигнализации "Буран-К2" (5800);</li> <li>- размыкатель компьютерных сетей "Буран-К3" (5800);</li> <li>- модуль дистанционного управления по проводному каналу «Буран-ДУ» (4500);</li> <li>- комплект дистанционной автоматической настройки «Буран-РК» с программным обеспечением (70000);</li> <li>- зашумляемый экран "Блок" на окно для защиты от утечки информации по оптико-электронному каналу</li> </ul> <p>- стоимость определяется конфигурацией остекления оконных проемов после заполнения бланка заказа установленной формы</p>	<ul style="list-style-type: none"> <li>- мониторинг уровня нагрузки каналов как в ходе настройки системы, так и в ходе эксплуатации;</li> <li>- контроль аварийных ситуаций и визуально-звуковая сигнализацию при отключении одного и более излучателей, коротком замыкании в канале помех, неисправности собственной системы вибрационного зашумления;</li> <li>- учет времени наработки под нагрузкой в часах и минутах;</li> <li>- защита от несанкционированного изменения настроек</li> </ul>
--	--	--	--	--	--

По результатам анализа в качестве устройства активной защиты была выбрана сертифицированная модель "Соната-АВ модель 4Б, поскольку она обладает сравнительной дешевизной и достаточно полной комплектацией с учетом отсутствия в защищаемом помещении окон, а также потенциально более высокой стойкостью защиты речевой информации вследствие статистической независимости возбуждения маскирующего шума во всех точках.

Блок электропитания и управления "Соната-ИП4.2", предназначен для электропитания, управления и настройки устройств Системы активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б. С подключённым пультом дистанционного управления "Соната-ДУ4.3" Изделие также обеспечивает управление блоком сопряжения "Соната-СК4.1" и средствами активной защиты информации от утечки за счёт ПЭМИН ("Соната-Р3", "Соната-Р3.1", "Соната-РС3") по интерфейсу ReBus-3.

### **6.3 Устройства для перекрытия электрического и электромагнитного каналов утечки информации**

В качестве методов защиты и ослабления электромагнитных полей используется установка электрических фильтров, применяются пассивные и активные экранирующие устройства и специальное размещение аппаратуры и оборудования. Установка экранирующих устройств может производиться либо в непосредственной близости от источника излучения, либо на самом источнике, либо, наконец, экранируется помещение, в котором размещены источники электромагнитных сигналов.

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. В качестве пассивной защиты помещений используются электромагнитные экраны, препятствующие прохождению волн.

Любой объект, который необходимо защитить от утечки информации, будь то помещение или оборудование, имеет определенный набор коммуникаций. В случае если применяется экранирование объекта, защиту от наводок на электрические цепи обеспечивают с помощью помехоподавляющих фильтров специальной конструкции. Они подавляют электромагнитные сигналы в широком диапазоне частот – от десятков килогерц до десятков гигагерц, при этом способ их монтажа на экран гарантирует радиогерметичность, защищая от потери эффективности экранирования. Помимо сетей электропитания, защита с помощью таких фильтров может быть обеспечена для различных сигнальных цепей, в том числе Ethernet, RS-232, USB и аудиосигналов.

Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой.

Защита от утечки информации через электромагнитные каналы может включать в себя применение Фарадеевских клеток, специальных материалов и экранирования для блокирования электромагнитных излучений. Это может предотвратить несанкционированный доступ к информации, передаваемой через электромагнитные волны.

Устройства для перекрытия данных каналов утечки информации приведены в таблице 6.2.



Таблица 6.3 - Устройства активной защиты электрического и электромагнитного каналов утечки информации

Модель	Минимальная цена, руб.	Диапазон рабочих частот, МГц	Сертификат	Состав системы	Особенности
ЛГШ-221	36400	0,01 - 1800	Сертификат ФСТЭК России № 3520 от 12 февраля 2016 года (до 12 февраля 2024 года)	Сетевой генератор шума «ЛГШ-221»	<ul style="list-style-type: none"> <li>- соответствует типу «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.</li> <li>- соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.</li> <li>- оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).</li> <li>- оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы. Изделия в режиме формирования маскирующих помех.</li> <li>- конструкция Изделия «ЛГШ-221» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</li> <li>- имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</li> </ul>
Соната-РС3	32400	-	Сертификат ФСТЭК России № 4493 от 09 декабря 2021 года (до 09 декабря 2026 года)	<ul style="list-style-type: none"> <li>- средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания "Соната-РС3" (32400);</li> <li>- блок электропитания и управления "Соната-ИП4.1" (26400);</li> <li>- блок электропитания и управления "Соната-ИП4.2" (36000);</li> <li>- блок электропитания и управления "Соната-ИП4.3" (21600);</li> </ul>	<ul style="list-style-type: none"> <li>- возможность регулирования уровня излучаемых электромагнитных шумов;</li> <li>- возможность блокировки прибора от несанкционированного доступа;</li> <li>- световой и звуковой индикаторы работы и контроля уровня излучения;</li> <li>- совместимость с проводными пультами ДУ линейки СОНАТА;</li> </ul>

				- пульт управления "Соната-ДУ4.3", опция (7680);	<ul style="list-style-type: none"> <li>- устройство для активной защиты информации от утечки по сети электропитания</li> <li>- предназначено для подключения к 3-проводной сети (энергосеть с проводом заземления);</li> <li>- звуковая и световая индикация работы;</li> <li>- возможно дистанционное управление посредством проводного пульта</li> </ul>
Соната-РК2	25960	0,01 - 2000	<p>Сертификат ФСТЭК России № 2168 от 13 сентября 2020 года (до 13 сентября 2019 года)</p> <p>Распространяется только на ранее установленные изделия*</p>	Устройство комбинированной защиты объектов информатизации от утечки информации по техническим каналам "Соната-РК2"	<ul style="list-style-type: none"> <li>- особенности конструкции "Соната-РК2" позволяют получать эффективное и недорогое решение задачи комплексной защиты ("ПЭМИ + наводки на ВТСС и их линии + наводки на линии электропитания и заземления") объекта вычислительной техники состоящего из одиночного средства вычислительной техники в ситуациях, когда остро стоит проблема помех, создаваемых генераторами маскирующего шума;</li> <li>- является комбинацией фильтра поглощающего типа, генераторов шумового тока с корректировкой спектра и регулировкой интегрального уровня и элементов антенной системы. При этом:</li> <li>- передаточная характеристика фильтра и частотный спектр мощности маскирующей помехи взаимно дополняют друг друга);</li> <li>- предусмотрена возможность избирательной корректировки спектральной плотности шума в 3-полосах с целью с целью минимизации ухудшения электромагнитной обстановки объекта;</li> <li>- обеспечивается "накачка" электромагнитной энергией шума элементов защищаемого технического средства (ТС) с целью создания помехи в комбинированных (и/или не учтенных) технических каналах "утечки" информации</li> </ul>

По результатам анализа в качестве устройства активной защиты было выбрано сертифицированное средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания "Соната-РС3". Данное устройство обладает приемлемой ценой и наиболее длительным периодом действия сертификата соответствия ФСТЭК.

## 6.4 Защита от ПЭМИН

Снижение уровня сигнала и создание условий, исключающих возможность его перехвата, становятся основными принципами борьбы с угрозами утечки информации по каналам ПЭМИН (Побочные ЭлектроМагнитные Излучения и Наводки).

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

Пассивные методы защиты информации в экранировании источника излучения технического средства, то есть СВТ размещается в экранированном шкафу или в экранированном помещении целиком. То есть экранируется каждое ТС входящее в состав нашего СВТ. В качестве недостатка такого метода можно выделить высокую стоимость экранированного помещения, если речь идет о нескольких СВТ и 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.

Для экранирования источника излучения применяются современные технологии, которые основаны на нанесении (например, напылении) различных специальных материалов на внутреннюю поверхность существующего корпуса, поэтому внешний вид компьютера практически не изменяется.

Активные методы защиты информации заключается в применении специальных широкополосных передатчиков помех. Метод хорош тем, что устраняется не только угроза утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы. Как правило, становится невозможным также и применение закладных подслушивающих устройств. Такие методы 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.

В качестве недостатков активных методов защиты можно выделить:

- вредность достаточно мощного источника излучения для здоровья;
- наличие маскирующего излучения свидетельствует, что в данном помещении есть защищаемые секреты, что само по себе привлекает к этому помещению повышенный интерес злоумышленников;
- при определенных условиях метод не обеспечивает гарантированную защиту компьютерной информации.

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 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. В помещениях, где установлены средства обработки защищаемой информации, были использованы генераторы шума в целях зашумления (радиомаскировки).

Устройства для перекрытия данных каналов утечки информации приведены в таблице 6.3.

Таблица 6.3 - Устройства активной защиты от ПЭМИН

Модель	Минимальная цена, руб.	Диапазон рабочих частот, МГц	Сертификат	Состав системы	Особенности
Соната-РЗ.1	42720	0,01 - 200	Сертификат ФСТЭК России № 3539 от 24 марта 2016 года (до 24 марта 2024 года)	<ul style="list-style-type: none"> <li>- средство активной защиты информации от утечки за счет ПЭМИН "Соната-РЗ.1" (33120);</li> <li>- антенна "Веер" (применяется для повышения уровней электромагнитного поля шума (ЭМПШ) в диапазоне частот 0,01...200 МГц) (9600);</li> <li>- (индивидуальный) пульт управления "Соната-ДУ4.4" с кабелем (комплекс 2320) (активация/деактивация и индикация работы в пределах одного выделенного помещения) (7680)</li> </ul>	<ul style="list-style-type: none"> <li>- соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты, может применяться в выделенных помещениях до 1 категории включительно;</li> <li>- изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "Соната-ДУ4.3" в комплексе с блоком питания "Соната-ИП4.х";</li> <li>- комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления);</li> <li>- наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений;</li> <li>- возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0.01...200 МГц за счет применения опционально поставляемой дополнительной антенны;</li> <li>- встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией;</li> <li>- возможность удаленного управления изделием как в случае автономного использования (непосредственно Пультом-ДУ4.2), так и в случае использования в составе комплекса ТСЗИ;</li> <li>- наличие счетчика наработки в режиме «Излучение».</li> </ul>
ЛГШ-503	44200	0,01 - 1800	Сертификат ФСТЭК России № 3519 от 12	Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-503» (44200)	<ul style="list-style-type: none"> <li>- соответствует требованиям документа «Требования к средствам активной защиты</li> </ul>

			февраля 2016 года (до 12 февраля 2024 года)		<p>информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты;</p> <ul style="list-style-type: none"> <li>- оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа);</li> <li>- оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех;</li> <li>- конструкция генератора обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним;</li> <li>- прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно- аппаратный комплекс «Паутина»</li> </ul>
Стикс-4	64200	0,01 - 1800 с возможностью расширения полосы до 2500	Сертификат ФСТЭК России № 3590 от 01 июля 2016 года (до 01 июля 2024 года)	<ul style="list-style-type: none"> <li>- Система защиты информации от утечки за счет ПЭМИН "Стикс-4";</li> <li>- Излучатель линейный</li> </ul>	<ul style="list-style-type: none"> <li>- предназначена для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок на объектах до 2-ой категории включительно</li> <li>- система осуществляет защиту информации от утечки: <ul style="list-style-type: none"> <li>- 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</li> <li>- 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</li> </ul> </li> </ul>

					<ul style="list-style-type: none"> <li>- равномерность огибающей спектра шумового сигнала в полосе до 1800 МГц с возможностью расширения полосы до 2500 МГц</li> <li>- высокая эффективность (соотношение излучаемой и потребляемой мощности) по сравнению с существующими аналогами</li> <li>- изделие выполнено в компактном форм-факторе блока питания со штепсельной вилкой и розеткой для подключения защищаемой вычислительной техники</li> <li>- система проста в установке и не требует проведения монтажных работ по установке внешних антенн</li> <li>- система обладает малым энергопотреблением, что позволяет, не создавая заметных нагрузок, запитывать ее от резервных источников питания</li> <li>- для наведения шумового сигнала на токопроводящие линии (за исключением линий электропитания) и инженерно-технические коммуникации необходимо использовать излучатель линейный (ИЛ)</li> <li>- система не создает акустического шума</li> </ul>
--	--	--	--	--	--

По результатам анализа в качестве устройства активной защиты была выбрана модель “Соната -Р3.1”. Данное устройство обладает неплохими характеристиками и при относительно невысокой цене является лучшим выбором среди конкурентов, поскольку может использоваться в комплексе "Соната-АВ" модель 4Б.



## 7 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В соответствие с вышеуказанными устройствами, выбранными в качестве средств обеспечения безопасности информации на предприятии, можно создать комплекс технических средств защиты информации "СОНАТА-АВ", включающий в себя:

- систему виброакустической защиты (СВАЗ);
- систему защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН);
- систему защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований с возможностью оперативного контроля исправности, режима работы и контроля состава комплекса (количество и тип устройств, входящих в комплекс).

Комплекс служит для защиты выделенного помещения и должен иметь возможность включения и выключения уполномоченным пользователем с помощью единого пульта управления, находящегося в выделенном помещении.

Дополнительные требования:

1. Информационный обмен между элементами комплекса допускается только по проводным линиям;
2. Должен быть возможен удаленный контроль состояния комплекса и управление комплексом оператором, находящимся вне выделенного помещения;
3. Должна быть предусмотрена возможность отдельной активации/деактивации 2 групп ТСЗИ. Например: группа 1 = СВАЗ + защита ТСС; группа 2 = защита от утечки по ПЭМИН.
4. Должна быть предусмотрена возможность оперативного выбора режима 1 из двух режимов работы СВАЗ:
  - a. "Аппаратура звукоусиления ВКЛючена" 
  - b. "Аппаратура звукоусиления ВЫКЛючена" 

Решение построено на базе системы защиты речевой информации от утечки по техническим каналам "Соната-АВ" модель 4Б включающее в себя блок электропитания и управления, излучатели, размыкатели, блоки сопряжения, пульт управления, а также САЗ от утечек за счет ПЭМИН, соединенные 3-проводной кабельной линией связи.

Информацию о режиме работы и исправности Системы "Соната-АВ" модель 4Б пользователь может получать как путем визуального наблюдения за сигнализацией на передней панели блока электропитания и управления "Соната-ИП4.1" ("Соната-ИП4.3")



(если есть техническая возможность), так и по светозвуковой индикации пульта "Соната-ДУ4.3".

Для удаленного контроля и управления комплексом ТСЗИ необходимо специализированное рабочее место.

Составим смету с учетом состава комплекса на базе оборудования "Соната", которая будет включать расходы на реализацию пассивных и активных мер защиты информации (Таблица 7.1).

Таблица 7.1 - Смета

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
<b>Комплекс "Соната-АВ" модель 4Б – локальное управление и удаленный мониторинг комплекса (СВАЗ + ПЭМИН + размыкатели)</b>			
<b>Электропитание и управление</b>			
Блок электропитания и управления "Соната-ИП4.2"	36000	1	36000
Пульт дистанционного управления "Соната-ДУ4.3"	7680	1	7680
<b>Система виброакустической защиты (СВАЗ)</b>			
Генератор-акустоизлучатель "СА-4Б"	7440	25	168000
Генератор-вибровозбудитель "СВ-4Б"	7440	53	394320
<b>Система защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН)</b>			
Средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок "Соната-РЗ.1"	42720	6	256320
Средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания "Соната-РСЗ"	32400	6	194400
<b>Система защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований</b>			
Размыкатель слаботочной линии "Соната-ВК4.2"	6000	9	54000
Размыкатель линии Ethernet "Соната-ВК4.3"	6000	9	54000
<b>3-х проводная линия связи</b>			
Кабель магистральный код 845 (бухта 50м). Предназначается для построения центральной магистрали системы	2880	1	2880
Кабель для отводов код 846 (бухта 50м). Предназначается соединения элементов системы с магистральной линией	3840	1	3840
Кабель с разъемом код 860. Длина 0,6 м. Предназначается для подключения излучателей, размыкателей к магистральной линии	300	1	300
Рулонная штора блэкаут на профиле	1600	11	17600
Звукоизоляционные, взломостойкие, огнестойкие дверные блоки серии "МТМ-ПРО-42"	24 000	2	48000
<b>ИТОГО</b>			<b>1237340</b>

Размещение устройств представлено на рисунке 7.1.



Рисунок 7.1 - Схема размещения инженерно-технических средств защиты

## **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: 22.10.2023  
[searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/](https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/).
2. Каналы утечки информации на предприятии - SearchInform. Дата просмотра: 22.10.2023  
[searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/kanaly-utechki-informatsii-na-predpriyatii/](https://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: 22.10.2023  
[learn.urfu.ru/resource/index/data/resource\\_id/40977/revision\\_id/0](https://learn.urfu.ru/resource/index/data/resource_id/40977/revision_id/0).