

**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»

Выполнил:

студент группы N34471

Буклеев Дмитрий Сергеевич

(подпись)

Проверил:

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

Студент	Буклеев Дмитрий Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии.
Задание	Проектирование инженерно-технической системы защиты информации на предприятии.

Краткие методические указания

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

Содержание пояснительной записки

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

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	Буклеев Дмитрий Сергеевич (Подпись, дата)

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

Студент Буклеев Дмитрий Сергеевич
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34471
10.03.01 (Технологии защиты информации 2019)

**Направление
(специальность)** Попов Илья Юрьевич
(Фамилия И.О)

Руководитель Инженерно-технические средства защиты информации
Проектирование инженерно-технической системы защиты
информации на предприятии.

Дисциплина

Наименование темы

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	21.09.2023	21.09.2023	
2.	Создание плана КР	22.09.2023	22.09.2023	
3.	Анализ теоретической составляющей	23.09.2023	23.09.2023	
4.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	26.09.2023	26.09.2023	
5.	Представление выполненной курсовой работы	05.12.2023	05.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Буклеев Дмитрий Сергеевич
(Подпись, дата)

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

Студент	Буклеев Дмитрий Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии.

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. 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 предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	Буклеев Дмитрий Сергеевич (Подпись, дата)

«__» _____ 20__ г.

Содержание

Термины и определения	6
Цели и задачи работы	8
Цели	8
Задачи	8
Введение	9
1. Анализ технических каналов утечки информации	11
2. Руководящие документы	16
3. Анализ защищаемых помещений	21
4. Анализ технических средств защиты информации	26
5. Описание расстановки технических средств	31
Заключение	33
Список использованных источников	34

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Коммерческая тайна – информация конфиденциального характера из любой сферы производственной и управленческой деятельности государственного или частного предприятия, разглашение которой может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем на основе государственных законодательных актов. Коммерческая тайна включает в себя также подробности коммерческой деятельности, состав партнеров, источники сырья, технологию сбыта продукции.

Промышленная тайна – это новые технологии, открытия, изобретения, применяемые в процессе производства продукции, и т. д.

Финансовая тайна - бухгалтерские и финансовые документы, деловая переписка и т. д.

Личная тайна – это сведения конфиденциального характера, разглашение которых может нанести материальный ущерб отдельному (физическому) лицу. Охрана личной тайны осуществляется ее владельцем. Государство не несет ответственность за сохранность личных тайн.

Документ – представленная на материальном носителе информация с идентификатором, позволяющим установить характер документа и его собственника.

Источник речевой информации - разговоры в помещениях и системы звукоусиления и звуковоспроизведения.

Носитель видовой информации объекта - сам объект, а также его фото- и видеоизображения на материальных носителях информации.

Политическая разведка - деятельность по добыванию сведений внутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства.

Экономическая разведка - сбор сведений, раскрывающих экономический потенциал определенной страны.

Военная разведка - сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники.

Научно-техническая разведка – сбор сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

Агентурная разведка - добывание информации и проведения диверсионных акций специально подобранных, завербованных и профессионально подготовленных агентов.

Легальная разведка-добыча информации при различных официальных связях и контактах с нашей страной, из легальных источников информации.

Техническая разведка - сбор информации с использованием технических разведывательных средств.

Воздушные каналы - каналы утечки информации, в которых средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Вибрационные каналы - каналы утечки информации, в которых средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

Акустоэлектрические каналы - каналы утечки информации, в которых утечка происходит за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами. Перехват акустических колебаний осуществляется через ВТСС, обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания».

Гидроакустический канал - канал, который образуется в водной среде и позволяет добывать акустическую информацию с использованием гидрофонов (сонаров).

Опτικο-электронный канал - каналы утечки информации, в которых утечка образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т. д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация).

Параметрические каналы - канал, в котором в результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС.

ЦЕЛИ И ЗАДАЧИ РАБОТЫ

Цели

Цель данной работы –повышение защищенности рассматриваемого помещения.

Задачи

1. Проанализировать защищаемое помещение;
2. Оценить каналы утечки информации;
3. Выбрать меры пассивной и активной защиты информации.

ВВЕДЕНИЕ

Для того чтобы построить эффективную систему противодействия утечке информации, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании физической природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы противодействия промышленному шпионажу позволит в дальнейшем выбирать оптимальные меры и средства защиты.

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

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющие линии, выходящие за пределы контролируемой зоны.

В качестве каналов утечки больше внимания следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны, а также посторонним проводам и кабелям, проходящим через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов. Интерес могут вызывать каналы утечки за счет вибраций, возникающих под давлением акустических волн, в твердых телах (ограждениях, трубах и т. п.).

Цели защиты информации от технических средств разведки на конкретных объектах информатизации определяются конкретным перечнем потенциальных угроз. В общем случае цели защиты информации можно сформулировать как:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах; • сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

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

1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Основными объектами защиты информации являются:

Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией;

Средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т. д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют объект ТСПИ.

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т. е. зоны с пропускной системой. Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1). Зона с возможностью перехвата

разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется опасной зоной. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной 1.



Рисунок 1 - Источники образования возможных каналов утечки информации

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, электромагнитными, акустическими и т. д. Они имеют в большинстве случаев колебательный характер, а информационными параметрами являются амплитуда, фаза, частота, длительность.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.

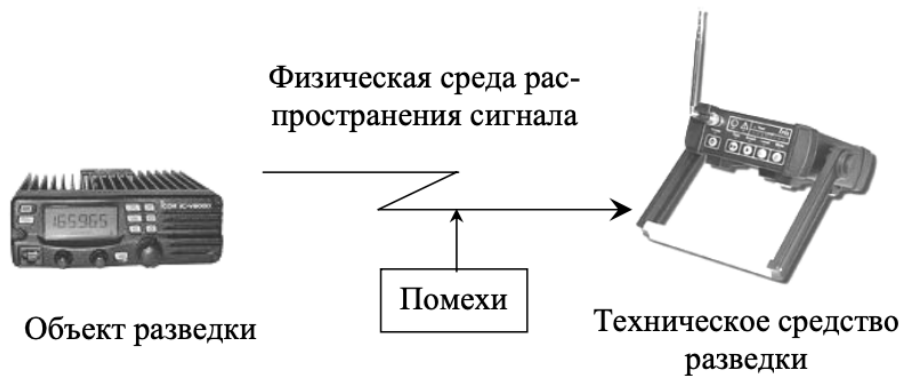


Рисунок 2 - Технический канал утечки информации (ТКУИ)

В зависимости от физической природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т. п.

Противодействие промышленному и экономическому шпионажу является непрерывным и адекватным новым типам угроз процессом развития методов, средств и способов защиты информации.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:

электромагнитные излучения элементов ТСПИ;

электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;

излучения на частотах самовозбуждения усилителей низкой частоты.

2. Электрические:

наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;

просачивание информационных сигналов в линии электропитания;

просачивание информационных сигналов в цепи заземления;

съем информации с использованием закладных устройств.

3. Параметрические:

перехват информации путем «высокочастотного облучения» ТСПИ.

4. Вибрационные:

соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2. Электрические каналы:

подключение к линиям связи.

3. Индукционный канал:

эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

среда распространения – воздух.

2. Виброакустические каналы:

среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:

результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:

преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:

облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами. Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съемка объектов. Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3. Съемка документов. Съемка документов осуществляется с использованием портативных фотоаппаратов



Рисунок 3 – Технические каналы утечки информации

2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Нормативные документы по противодействию технической разведке:

1. Законы Российской Федерации:

«О государственной тайне» от 21 июля 1993 г. №5151–1.

«Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ.

«О безопасности» от 5 марта 1992 г. №2446–1.

«О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1.

«О связи» от 16 февраля 1995 г. №15-ФЗ.

«Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

2. Указы Президента Российской Федерации:

«Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212.

«Вопросы защиты государственной тайны» от 30.03.1994 г. №614.

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.

«О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.

«Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594.

«О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644.

«Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

3. Постановления Правительства Российской Федерации:

Инструкция №0126–87.

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921-51.

«Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233.

«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333.

«О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513.

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.

«Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973.

«О сертификации средств защиты информации» от 26 июня 1995 г. №608.

4. Решения Гостехкомиссии России:

«Основы концепции защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам» от 16 ноября 1993 г. № 6.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации» от 14 марта 1995 г. № 32.

«Типовое положение о Совете (технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам» от 14 марта 1995 г. № 32.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (учреждении, организации)» от 14 марта 1995 г. № 32.

«О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте» от 3 октября 1995 г. № 42.

«Методические рекомендации по разработке развернутых перечней сведений, подлежащих засекречиванию» от 3 февраля 1995 г. № 29.

«Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)» от 23 мая 1997 г. № 55.

«Положение о государственном лицензировании деятельности в области защиты информации (Решение Гостехкомиссии России и ФАПСИ)» от 27 апреля 1994 г. № 10 с дополнениями и изменениями, внесенными Решением Гостехкомиссии России и ФАПСИ от 24 июня 1997 г. № 60.

Положение о головной научно-исследовательской организации по проблеме защиты информации (Решение Председателя Гостехкомиссии России) от 15 марта 1993 г.

Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР (Пособие к ВСН-01-82). Утверждено НИИА и согласовано с Гостехкомиссией СССР в 1983 г., переутверждено Решением Гостехкомиссии России от 13 ноября 1990 г, № 89–3.

«О защите информации при вхождении России в международную информационную систему «Интернет» от 21 октября 1997 г. № 61.

5. Руководящие и нормативно-методические документы Гостехкомиссии России:

Руководящий документ (РД). Защита от несанкционированного доступа (НСД) к информации. Термины и определения. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по ЗИ. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

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

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

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

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

Модель ИТР-2010. Решение Гостехкомиссии России от 16 августа 1996 г. № 49.

Методики оценки возможностей ИТР (МВТР-87) (с изменениями) Решение Гостехкомиссии СССР от 16 сентября 1987 г. №70-3, извещения № 1-88, № 2-90, № 3-91, № 4-93.

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

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

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

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

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

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

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

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

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

Нормативно-методические документы по противодействию средствам иностранной акустической (речевой) разведки. Решение Гостехкомиссии России. 1991 г.

Нормы эффективности защиты АСУ и ЭВТ от утечки информации за счет ПЭМИН. Решение Председателя Гостехкомиссии СССР, 1977 г.

Нормы эффективности защиты технических средств передачи телевизионной информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13, от 30 ноября 1987г. № 11-3.

Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13.

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Наименование организации: ООО «БиоБаланс»

Область деятельности: биотехнологии

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

Основные информационные процессы:

- 1) Публикация предложения услуг
- 2) Предоставление пользователям инструментов для заказа услуги и создания учётной записи на сайте
- 3) Технологическое сопровождение оказания услуги
- 4) Предоставление консультаций пользователям
- 5) Удаление данных по завершении сотрудничества
- 6) Ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией
- 7) Хранение, обработка, передача, утилизация персональных данных пользователей
- 8) Хранение данных о биоматериале, сданном клиентами
- 9) Хранение данных о внутренних биотехнологических разработках
- 10) Внутреннее взаимодействие департаментов методами асинхронной коммуникации

Основные информационные потоки:

- 1) Открытые потоки: взаимодействие с отделом управления проектами, взаимодействие с отделом клиентского управления (служба поддержки, отдел по работе с ключевыми клиентами, отдел предоставления услуг), взаимодействие с отделом маркетинга, взаимодействие со службой контроля качества.
- 2) Закрытые потоки: взаимодействие с отделом клиентского управления (финансовый отдел), взаимодействие с отделом биоисследований, взаимодействие с отделом технического управления (Круглосуточная дежурная служба, отдел информационной безопасности, отдел системного администрирования).

Информация ограниченного доступа:

1) Персональные данные сотрудников – является информационным активом, представлены в электронной форме, владельцем является руководитель отдела, отдел кадров.

2) Персональные данные клиентов - является информационным активом, представлены в электронной форме, владельцем является сотрудники отдела технической поддержки с необходимым уровнем доступа

3) Биоматериал клиентов

4) Техническая информация (логины, пароли, данной локальной сети и т. д.) - является информационным активом, представлены в электронной форме, владельцем являются сотрудники отдела технической поддержки с необходимым уровнем доступа.

5) Коммерческая тайна (сайт, CRM-система) – является информационным активом, представлен в электронной форме, владельцем является Компания.

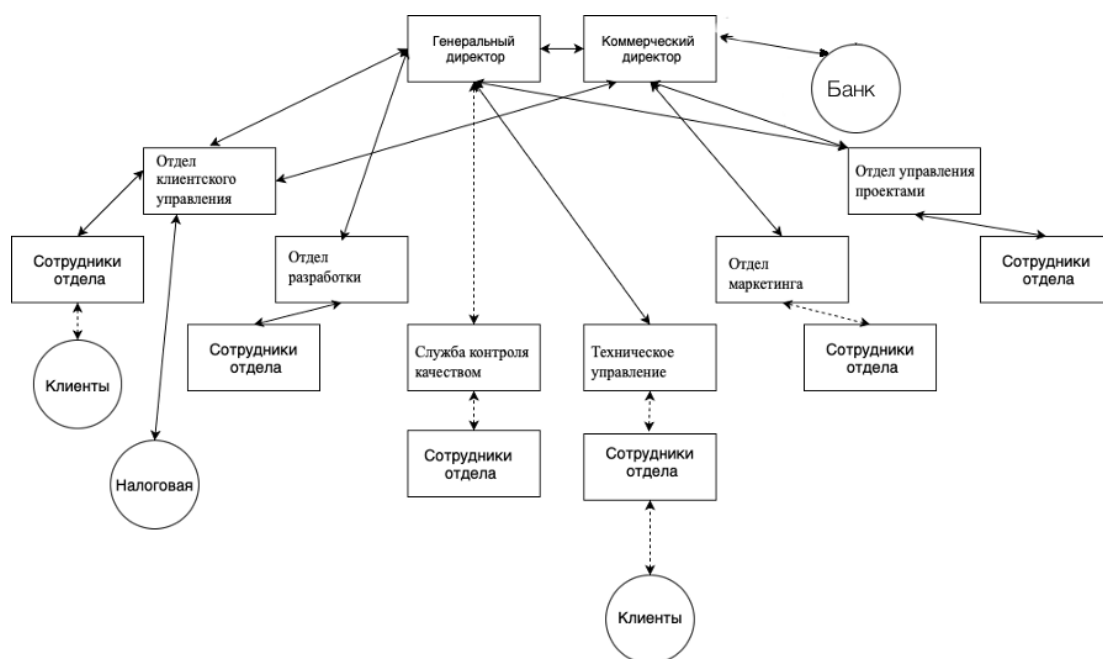


Рисунок 4 – Основные информационные потоки

Система имеет классификацию «секретно», т.е. к секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесённый интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности. Соответственно система имеет 3 тип формы доступа-для граждан, допускаемых к секретным сведениям.

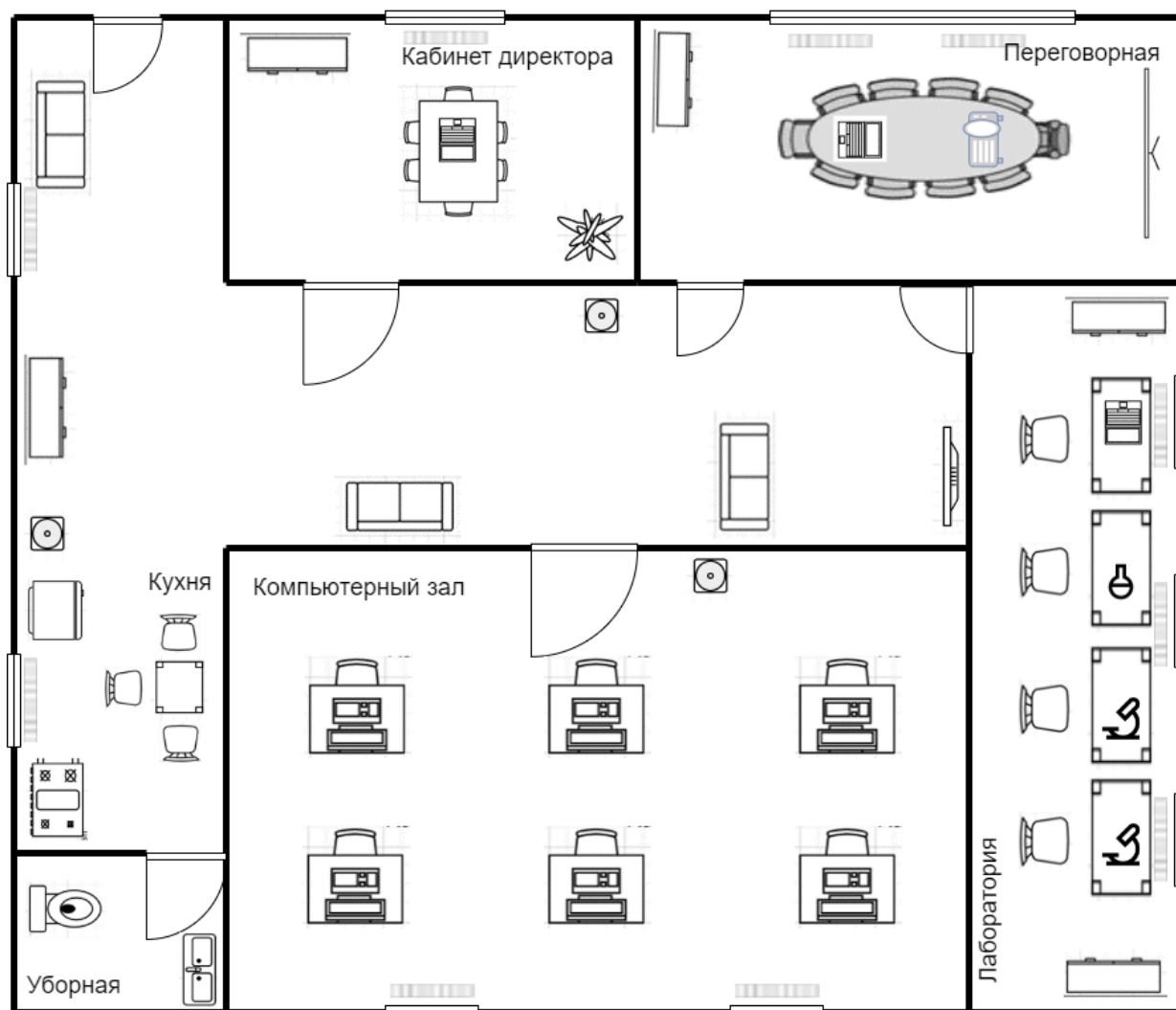



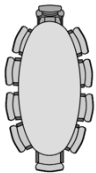



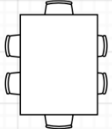





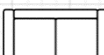







Рисунок 5 – План помещения

Обозначение	Описание
	Батарея-радиатор
	Экран для проектора
	Проектор

	Стол для переговоров
	Растение
	Кулер
	Ноутбук
	Стол директора
	Лабораторное оборудование
	Стол
	АРМ
	Шкаф
	Стул
	Диван
	Телевизор
	Плита
	Раковина
	Холодильник
	Туалет

Помещения, требующие защиты:

Переговорная: 10.04 м на 6.30м – 63.3м²

Кабинет директора: 6.2 м на 6.3м – 39м²

Компьютерный зал: 11 м на 10.30м – 113.3м²

Лаборатория: 3.78 м на 13.30м – 50.2м²

Для ведения переговоров предназначено два помещения (кабинет директора и переговорная). В переговорной находятся: стол, 10 стульев, проектор, экран для проектора, компьютер, 2 розетки, 2 батареи центрального отопления. В кабинете директора: стол, 6 стульев, ноутбук, 2 розетки, батарея центрального отопления, шкаф, растение. В компьютерном зале 2 окна, 2 батареи ЦО, 6 рабочих мест с АРМ, 12 розеток, кулер. В лаборатории установлено 4 стола с химическим оборудованием, 2 шкафа, 3 окна и 3 батареи центрального отопления. Помещение расположено на 3 этаже малоэтажного 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. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к секретным сведениям. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

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

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствами защиты, приведенными в таблице 1.

Таблица 1. Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустический акустоэлектрический	Проводка, двери, окна	Сетевые фильтры, звукоизоляция кабинета директора и переговорной	Акустическое зашумление
вибрационный виброакустический	Батареи и трубы, стены, пол, окна, двери	Изолирующие звук и вибрацию материалы стен	Вибрационное зашумление
оптический	Окна, двери	Жалюзи/шторы на окнах, доводчики на двери	Блокирующие обзор устройства
электромагнитный электрический	АРМ, ноутбуки, бытовые приборы, телевизоры, розетки	Сетевые фильтры	Электромагнитное зашумление

4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.

3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.

4. Все режимные помещения оборудуются аварийным освещением.

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

Устройства противодействия утечке информации по акустическому и виброакустическому каналам

Пассивная защита представляет собой:

- Усиленные двери;
- Сетевые фильтры

- Изолирующие звук и вибрацию материалы стен

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б. Ниже в таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналам.

Таблица 2. Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, руб
Портативный генератор акустического шума ЛГШ-303	Диапазон рабочих частот 180 ÷ 11 300 Гц	Изделие предназначено для защиты речевой информации от перехвата по прямому акустическому каналу.	15 600
Генератор акустического шума ЛГШ-304	Диапазон рабочих частот 175 ÷ 11 200 Гц	Сертификат ФСТЭК РОССИИ по 2 классу защиты; может устанавливаться в ВП до 2 категории	25 220
SI-3030 Виброакустический шумогенератор	Спектр шумовой помехи 125 Гц - 6,3 кГц	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции.	28 500
"ANG-2200" - генератор шума	Диапазон акустического шума 250 Гц...5 кГц	Генератор шума для акустического зашумления помещения и его защиты от утечки информации по виброканалам (250...5000 Гц). Сертификат Гостехкомиссии.	18 000
«БУБЕН» - генератор акустической помехи	Диапазон рабочих частот 400...18000 Гц	Используется для защиты конфиденциальных переговоров по принципу создания акустических помех. Вид помех: речеподобная, "белый шум".	15 000
SpyLock Jack - устройство блокирования утечки информации по акустическому каналу	Подходит для iPhone, Samsung и других аппаратов. Разъем 3.5 mm.	Устройство предназначено для защиты речевой информации путем блокирования микрофонов и динамиков мобильного телефона на механическом и программном уровне.	15 000
Фотон-М - устройство защиты оптоволоконной линии от утечки акустической информации	Скорость передачи данных в сетях по технологии Ethernet до 100 Мбит/с	Устройство защиты акустической речевой информации от утечки по волоконно-оптической линии связи (ВОЛС).	395 000
Антенна 3 ГГц пассивная двухкомпонентная ПА-111	-	Антенна ПА-111 позволяет формировать в пространстве как магнитную (в диапазоне от 0,01 до 30 МГц), так и электрическую (в диапазоне от 0,01 до 3000 МГц) составляющие электромагнитного поля шума. Конструкция предусматривает возможность установки на ней генераторов ГШ-111У или ГШ-111П системы «Шифон» и возможность крепления на вертикальные поверхности (стены).	-
Упрощенный вариант генератора ГШ-111У	В комплект поставки входит генератор ГШ-111У и ПО конфигурирования системы / Дополнительно к	Упрощенный вариант генератора шума без кнопочной клавиатуры и ЖКИ. Управление, регулировка и контроль осуществляются только через компьютер по сети Ethernet.	75 000

	генератору можно приобрести: Антенна 6 ГГц активная АА-6000, Антенна 3 ГГц пассивная двухкомпонентная ПА-111		
Буран-2	Диапазон рабочих частот не менее 180-11200 Гц	Система акустических и виброакустических помех «Буран-2» является средством активной акустической и вибрационной защиты акустической речевой информации, соответствует требованиям ФСБ России к разработке, производству, сертификации и эксплуатации технических средств защиты особо важных и выделенных помещений органов государственной власти по виброакустическому каналу утечки речевой информации и может использоваться для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, циркулирующей в выделенных помещениях до 2 категории включительно.	81 000
Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б	Диапазон частот до 2 ГГц, диапазон регулировки	Генератор шума. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы.	23 000
БУБЕН-УЛЬТРА (Исп. «ЛЮСТРА») - подавитель диктофонов и микрофонов увеличенной мощности, встроенный в подвесной динамик системы оповещения.	24 ультразвуковых излучателя	Самый мощный прибор из представленных на рынке! Ультразвуковая помеха не слышима. Повышенная дальность подавления за счёт «know how» производителя. Два вида сложной помехи: сложная ультразвуковая помеха. Крепиться к потолку над столом переговоров. Имеет возможность регулировки по высоте.	65 000

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

Устройства противодействия утечке информации по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи или шторы. С точки зрения удобства содержания были выбраны жалюзи.

Устройства противодействия утечке по электромагнитным и электрическим каналам

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. Устройства активной защиты представлены в Таблице 3.

Таблица 3. Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, руб
SEL SP-44 Устройство защиты цепей электросети и заземления	Спектральная плотность напряженности электрического поля шума 0,01 - 1 МГц 90 дБ / 1 - 10 МГц 70 дБ / 10 - 100 МГц 50 дБ / 100 - 300 МГц 35 дБ	Генератор зашумления электросети 220 В и цепи заземления	24 000
ФСП-1Ф-7А Фильтр сетевой помехоподавляющий	Напряжение питания 220В	ФСП-1Ф-7А Фильтр сетевой помехоподавляющий	15 300
Фильтр сетевой помехоподавляющий ФСПК-40	Напряжение питания 220/380 В ± 10%, 50 Гц	Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети.	70 500
"СОНАТА-ФС10.1"	Защищаемая линия электропитания Однофазная, номинальное напряжение 220 В, частота 50 Гц	ТСЗИ "Соната-ФС10.1" (далее – Изделие) предназначено для защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных наводок информативного сигнала на линии электропитания напряжением 220 В с частотой 50 Гц.	32 400
Фильтр сетевой помехоподавляющий ФСПК-200	Напряжение питания 220/380 В ± 10%, 50 Гц	Фильтр сетевой помехоподавляющий ФСПК-200-0,22/0,38-91-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети.	315 000
ЛРЧФ-100-1Ф	Диапазон рабочих частот 0,15 - 40 000 МГц	Изделие «ЛРЧФ-100-1Ф» предназначено для исключения или затруднения получения иностранной радио-, радиотехнической разведкой охраняемых параметров образцов вооружения и военной техники (ВиВТ) на технологических рабочих местах путем ограничения электромагнитной энергии опасного сигнала внутри замкнутых экранов в линиях электропитания напряжением до 380 В. Изделие «ЛРЧФ-100-1Ф»	83 200

		является пассивным техническим средством противодействия иностранной радио-, радиотехнической разведке.	
--	--	---	--









По результатам анализа была выбрана система "СОНАТА-ФС10.1". Кроме того, что она является наиболее популярным решением для этого класса защиты (отмечена как «хит продаж» на нескольких сайтах-агрегаторах), она сочетает в себе умеренную стоимость с большим диапазоном. Так же предлагается приобрести сетевой фильтр ФСП-1Ф-7А.

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Согласно информации, приведённой в 4 главе, выбранные средства защиты информации включают в себя:

- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт., в переговорную, кабинет директора, лабораторию и компьютерный зал.
- Жалюзи на 9 окон.
- «БУБЕН» - генератор акустической помехи
- "СОНАТА-ФС10.1"
- ФСП-1Ф-7А Фильтр сетевой помехоподавляющий
- РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.1 для защиты телефонной линии

Таблица 4. Смета

Устройство	Цена, руб	Кол-во	Обозначение	Стоимость, руб
Blackout-жалюзи 2х3м	5280	9	-	47 520
Усиленные звукоизолирующие двери Ultimatum PP	75 283	4		301 132
«БУБЕН»	15 000	2		30 000
Вибропреобразователь для окон ЛВП-2о	3600	7		25 200
Акустический излучатель «ЛВП-2а»	3600	8		28 800
Вибропреобразователь «ЛВП-2с»	3600	19		68 400
РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.1	6000	1		6000
Генератор шума "Гамма-ГШ18"	31 500	4	  	126 000
"СОНАТА-ФС10.1"	32 400	3		97 200

ФСП-1Ф-7А помехоподавляющий	Фильтр сетевой	15 300	1	ФСП	15 300
ИТОГО					745 552

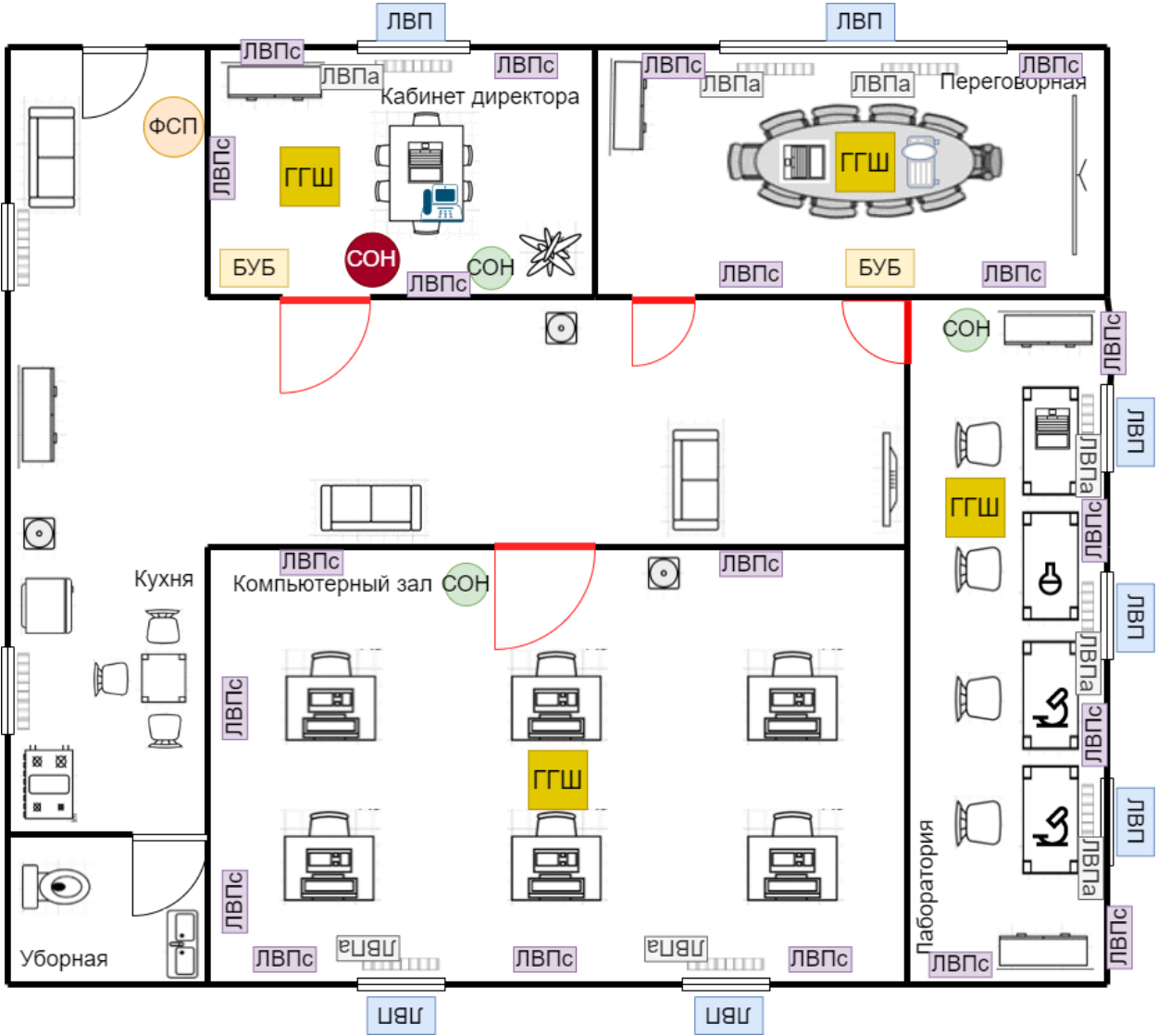


Рисунок 6 – Схема расстановки устройств

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. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)