

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

Факультет безопасности информационных технологий

Дисциплина:

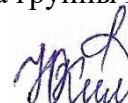
«Инженерно-технические средства защиты информации»

Курсовая работа

«Разработка комплекса инженерно-технической защиты информации в помещении»

Выполнила:

Килина Ю. А., студентка группы N34471



(подпись)

Проверил:

к.т.н., доцент ФБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Килина Юлия Алексеевна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34471
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении
Задание	Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

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

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Килина Юлия Алексеевна 
	(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Килина Юлия Алексеевна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34471

Направление (специальность) 10.03.01. - Технологии защиты информации


Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу и аннотации	15.11.2023	15.11.2023	
2	Изучение теоретического материала	30.11.2023	30.11.2023	
3	Написание основного текста курсовой работы	10.12.2023	17.12.2023	
4	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Килина Юлия Алексеевна 
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Килина Юлия Алексеевна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34471
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☒ Предложены студентом ☐ Сформулированы при участии студента
☐ Определены руководителем

Цель данной работы – исследовать способы предотвращения утечек конфиденциальной информации через технические каналы связи.

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое

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 выполнения работы был проведён анализ каналов утечки информации, были изучены активные и пассивные методы защиты информации, проведена классификация технических каналов утечки информации, предложены меры защиты информации от утечек по техническим каналам

Руководитель	Попов Илья Юрьевич	(Подпись, дата)
Студент	Килина Юлия Алексеевна	(Подпись, дата)

«___» _____ 2023 г

СОДЕРЖАНИЕ

Введение	6
1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	7
2 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	10
3 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ	15
4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	17
4.1 Анализ возможных утечек информации	21
4.2 Выбор средств защиты информации	21
5 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.....	23
Устройства для перекрытия акустического и виброакустического каналов утечки информации	23
5.1 Устройства противодействия утечке информации по оптическому каналу.....	27
5.2 Устройства противодействия утечке по электромагнитным и электрическим каналам.....	27
Заключение.....	33
Источники	34

ВВЕДЕНИЕ

В настоящее время информационная безопасность является одной из важнейших задач для организаций, государственных учреждений и частных лиц. С развитием информационных технологий возрастает угроза утечек информации через технические каналы. Организации вкладывают средства в современные технологии и передовые исследования, чтобы оставаться конкурентоспособными на рынке. Любое разглашение конфиденциальной информации, например, утечка персональных данных, бухгалтерских отчётов, коммерческой тайны, технологических разработок и секретов производства может привести к потере репутации и доверия со стороны клиентов и партнёров, значительным финансовым убыткам.

Ряд учреждений может обрабатывать данные, содержащие государственную тайну, в том числе политические сведения, данные о военных операциях, сведения о промышленном комплексе, контроле за экспортом и других вопросах, касающихся национальной безопасности. Утечка таких данных может нанести серьёзный ущерб интересам государства и повлечь за собой риск для жизни и здоровья граждан.

Согласно аналитическому отчёту компании InfoWatch, в 2022 году количество утечек информации выросло на 112% по сравнению с результатами 2021 года. По данным компании Солар от 19 октября 2023 года в России государственный сектор и крупный бизнес теряют около 5,5 млн рублей в результате одной утечки. В связи с этим, вопросы предотвращения утечек информации и обеспечения информационной безопасности становятся ключевыми задачами для бизнеса и государства.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации.

Цель работы – исследовать способы предотвращения утечек конфиденциальной информации через технические каналы связи.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести классификацию технических каналов утечки информации;
- провести анализ защищаемого помещения;
- изучить пассивные и активные способы защиты;
- провести анализ рынка инженерно-технических средств защиты информации;
- разработать систему инженерно-технической защиты информации на основе выбранных средств защиты.

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Утечка — бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Физический путь переноса информации от её источника к несанкционированному получателю называется каналом утечки. Если запись информации на носитель канала утечки и съём её с носителя осуществляется с помощью технических средств, то такой канал называется техническим каналом утечки.

Утечка (информации) по техническому каналу — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический канал утечки информации, так же, как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника (рисунок 1).



Рисунок 1 – Структура технического канала утечки информации

Информация передается полем или веществом. Это может быть либо акустическая волна, либо электромагнитное излучение, либо лист бумаги с текстом и т.п. Другими словами, используя те или иные физические поля, человек создает систему передачи информации или систему связи. Система связи в общем случае состоит из передатчика, канала передачи информации, приёмника и получателя информации. Легитимная система связи создается и эксплуатируется для правомерного обмена информацией. Однако ввиду физической природы передачи информации при выполнении определенных условий возможно возникновение системы связи, которая передает информацию вне зависимости от желания отправителя или получателя информации — технический канал утечки информации.

Технический канал утечки информации (ТКУИ) — совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от её источника или с выхода предыдущего канала. В качестве источника сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись её на носитель информации, соответствующий среде распространения. В общем случае он выполняет следующие функции:

- создаёт поля или электрический ток, которые переносят информацию;
- производит запись информации на носитель;
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Среда распространения сигнала — физическая среда, по которой информативный сигнал может распространяться и регистрироваться приёмником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Среда может быть однородная и неоднородная. Однородная — вода, воздух, металл и т. п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Приёмник выполняет функцию, обратную функции передатчика. Он производит:

- выбор носителя с нужной получателю информацией;

- усиление принятого сигнала до значений, обеспечивающих съём информации;
- съём информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Таким образом, описание ТКУИ должно включать в себя:

- источник угрозы (приёмник информативного сигнала);
- среду передачи информационного сигнала;
- источник (носитель) информации.

2 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Технические каналы утечки информации классифицируются в соответствии с физической природой их проявления и методами обнаружения.

По физической природе носителя и виду канала связи ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;
- акустоэлектрические;
- виброакустические;
- материально-вещественные.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
- большой объем добываемой информации;
- оперативность получения информации вплоть до реального масштаба времени;
- скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация, видовые и сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по телефону;

- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;
- приёмника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Перехват акустической информации может происходить не только в помещении или в транспорте, существуют риски утечки даже при разговоре на улице. Шум оживленной трассы или включение воды в номере гостиницы не подавят сигнал, нужны специальные устройства, снижающие риск передачи данных в воздушной среде по каналам утечки акустической информации.

Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нём вибрационных колебаний в результате виброакустического преобразования. Эти колебания, распространяющиеся в твёрдой среде, могут быть перехвачены специальными средствами разведки, а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. С этой целью используют устройства, преобразующие вибрационные колебания в электрические сигналы, соответствующие соответствующим звуковым частотам. Такие устройства называются вибродатчиками. Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушан, зарегистрирован на магнитном или другом носителе или передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному каналу передачи информации.

В целях ведения разведки с использованием виброакустического канала широко применяются стетоскопы, т.е. устройства, содержащие вибродатчик (стетоскопный микрофон), блок обработки сигнала, осуществляющий его усиление и ослабление помех, и головные телефоны. В ряде таких устройств предусмотрена возможность записи сигнала на магнитный носитель. Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Вибродатчик обычно крепится к металлическому предмету вмонтированного в стену. В качестве звукопровода могут использоваться трубы водоснабжения, канализации, батареи отопления и т.д. На качество приема вибросигналов кроме свойств вибродатчика и материала твердой среды влияют ее толщина, а также уровни фоновых акустических шумов в помещении и вибраций в твёрдой среде.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические

колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи. Защита осуществляется посредством использования специальных программных и аппаратных средств, позволяющих выявить закладки.

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно:

- побочные электромагнитные излучения, возникающие вследствие протекания по элементам технических средств приёма, обработки, хранения и передачи информации (ТСПИ) и их соединительным линиям переменного электрического тока;
- побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
- побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители на магнитных носителях;
- чтение информации с накопителей на магнитных носителях;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства – принтеры, плоттеры;
- запись данных от сканера на магнитный носитель (ОЗУ).

Материально-вещественный канал утечки информации

Особенность этого канала вызвана спецификой источников и носителей информации по сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты (макро и микрочастицы), которые имеют четкие пространственные границы локализации, за исключением излучений радиоактивных веществ. Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Для более четкого описания рассматриваемого канала целесообразно уточнить состав источников и носителей информации.

Основными источниками материально-вещественного канала утечки информации являются следующие:

- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся на предприятии (организации);
- отходы делопроизводства и издательской деятельности на предприятии (организации), в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;
- нечитаемые дискеты ПЭВМ из-за их физических дефектов и искажений загрузочных или других кодов;
- бракованная продукция и ее элементы;
- отходы производства в газообразном, жидком и твердом виде.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами:

- сотрудниками организации и предприятия;
- воздушными массами атмосферы;
- жидкой средой;
- излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках - в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т. д.; демаскирующие - в газообразных, жидких и твердых отходах производства.

Объект наблюдения в оптическом канале утечки информации является одновременно источником информации и источником сигнала в том смысле, что световые

лучи, несущие информацию о видовых признаках объекта, представляют собой отраженные объектом лучи внешнего источника или его собственные излучения.

Отраженный от объекта свет содержит информацию о его внешнем виде (видовых признаках), а излучаемый объектом свет - о параметрах излучений (сигнальных признаках). Запись информации производится в момент отражения падающего света путем изменения яркости и спектрального состава отраженного луча света. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения.

В общем случае объект наблюдения излучает электромагнитные волны и отражает свет другого источника как в видимом, так и ИК-диапазонах. Однако в конкретных условиях соотношения между мощностью собственных и отраженных излучений в видимом и ИК-диапазонах существенно отличаются.

В видимом диапазоне мощность излучения определяется в подавляющем большинстве случаев мощностью отраженного света и содержащихся в объекте искусственных источников света.

Оптический канал утечки информации реализуется непосредственным восприятием глазом человека окружающей обстановки путем применения специальных технических средств, расширяющих возможности органа зрения по видению в условиях недостаточной освещенности, при удаленности объектов наблюдения и недостаточности углового разрешения. Это и обычное подглядывание из соседнего здания через бинокль, и регистрация излучения различных оптических датчиков в видимом или ИК-диапазоне, которое может быть модулировано полезной информацией. При этом очень часто осуществляют документирование зрительной информации с применением фотопленочных или электронных носителей. Наблюдение дает большой объем ценной информации, особенно если оно сопряжено с копированием документации, чертежей, образцов продукции и т. д. Процесс наблюдения сложен, так как требует значительных затрат сил, времени и средств.

Характеристики всякого оптического прибора (в т. ч. глаза человека) обуславливаются такими первостепенными показателями, как угловое разрешение, освещенность и частота смены изображений. Большое значение имеет выбор компонентов системы наблюдения. Наблюдение на больших расстояниях осуществляют объективами большого диаметра. Большое увеличение обеспечивается использованием длиннофокусных объективов, но тогда неизбежно снижается угол зрения системы в целом.

3 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;
- МЕЖВЕДОМСТВЕННАЯ КОМИССИЯ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ 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";

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

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;

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

4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

На рисунке 2 представлен план защищаемого помещения.

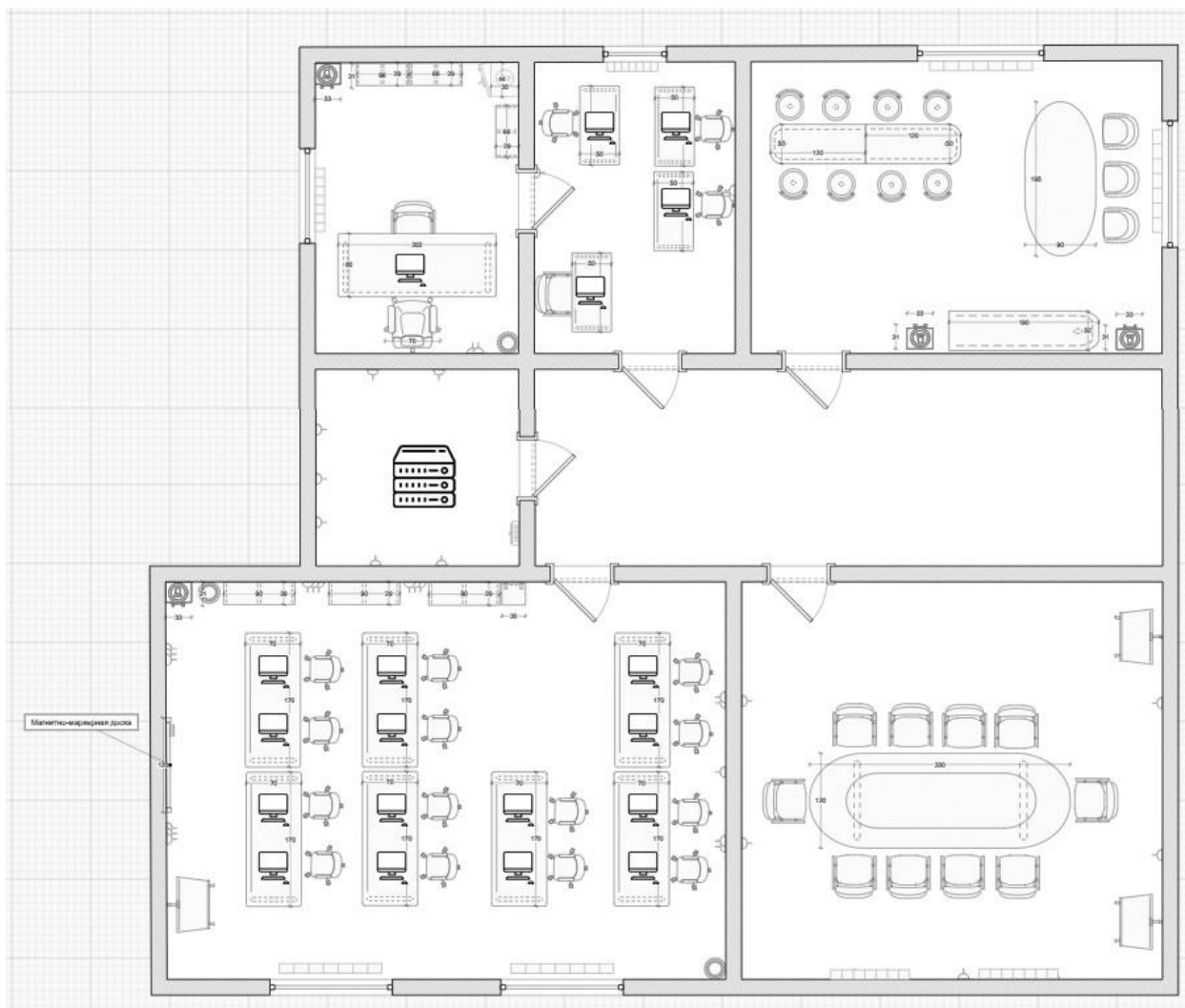




Рисунок 2 – План защищаемого помещения

Таблица 1 – Используемые обозначения

Обозначения	Описание
	Кресло руководителя
	АРМ













	Кресло для переговорной
	Офисное кресло
	Флипчарт
	Обеденный стол
	Барная стойка
	Кулер
	Офисный стол
	Барный стул
	Шкаф для бумаг
	Сейф
	Урна
	Тумбочка

Схема информационных потоков представлена на рисунке 3.

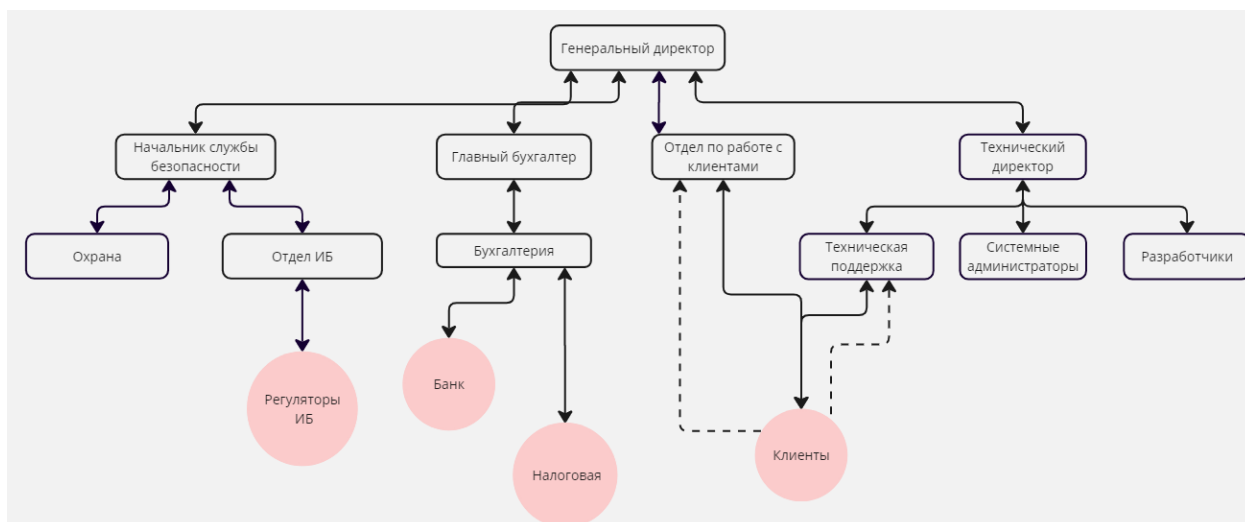


Рисунок 3 – Схема информационных потоков

Описание информационных потоков

	Закрытые информационные источники
	Открытые информационные источники

Информация ограниченного доступа:

1. Персональные данные сотрудников – является информационным активом, представлены в электронной форме, владельцем является руководитель службы безопасности, отдел информационной безопасности.
2. Персональные данные клиентов - является информационным активом, представлены в электронной форме, владельцем являются сотрудники отдела по работе с клиентами с необходимым уровнем доступа
3. Конфигурация ПО клиентов - является информационным активом, представлена в электронной форме, владельцем являются сотрудники ИТ-отдела.
4. Техническая информация (логины, пароли, данной локальной сети и т. д.) - является информационным активом, представлены в электронной форме, владельцем являются сотрудники ИТ-отдела с необходимым уровнем доступа.
5. Коммерческая тайна (данные о производстве) – представлен в электронной форме, владельцем является владелец Организации.
6. Финансовые данные, данные о состоянии счетов, доходов и расходов – являются информационным активом, представлены в электронной форме, владельцем

является главный бухгалтер.

Система имеет классификацию «секретно», т.е. к ней относятся все сведения, не относящиеся к сведениям с грифом «особой важности» и «совершенно секретно», но составляющие государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

3.1 Описание помещений

Защите подлежат следующие помещения:

- кабинет директора 9,49 м²;
- офис 9,39 м²;
- переговорная комната 26,84 м²;
- кофе-пойнт 19,28 м²;
- open space 35,68 м²;
- серверная 6,5 м²;
- коридор 20,05 м².

В переговорной комнате нет окон и средств вычислительной техники. Вход в кабинет директора осуществляется через бухгалтерию. В серверной нет окон.

В open space есть 7 рабочих столов, магнитно-маркерная доска, 14 офисных кресел, 2 окна с батареями центрального отопления, 17 розеток, есть 3 шкафа для бумаг, кулер, тумба, 2 мусорных корзины. Из средств вычислительной техники в помещении установлены ПЭВМ, включённые в локальную сеть. В кофепойнте есть 2 окна с батареями центрального отопления, 3 барных стола, 8 барных стульев, обеденный стол, 3 обеденных стула, кофемашина и кулер.

В бухгалтерии есть 1 окно с радиатором центрального отопления, 4 рабочих стола, 4 компьютерных стула, 4 ПЭВМ.

В кофепойнте есть 3 барных стойки, 8 барных стульев, обеденный стол, 3 обеденных стула, 2 кулера, 2 окна с радиаторами центрального отопления.

4.1 Анализ возможных утечек информации

Из-за расположения помещения на втором этаже возможен просмотр его извне, как с улицы, так и со стороны жилого дома с использованием оптических приборов, что создает потенциальную возможность утечки видовой информации.

Из-за возможности прослушивания помещения через открытые окна и форточки с помощью направленных микрофонов с улицы или из жилого дома, может произойти существует потенциальный акустический канал утечки информации.

При использовании лазерного микрофона в жилом доме для перехвата разговоров можно получить информацию о проводимых в помещении беседах через вибрации оконных стекол. Таким образом, существует еще один способ утечки акустической информации.

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.

4.2 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 2.

Таблица 2 – Активная и пассивная защита

Каналы	Источники	Пассивная защита	Активная защита
Акустический и акустоэлектрический	– окна – двери – электрическая сеть	– звукоизоляция переговорной и кабинета директора – установка сетевых фильтров – закрытие окон и дверей во время планёрок, совещаний, переговоров	– устройства акустического зашумления – генератор белого шума

Вибрационный и виброакустический	<ul style="list-style-type: none"> – все твердые поверхности помещения – батареи – вентиляц ия – трубы – окна – двери 	<ul style="list-style-type: none"> – дополнительное помещение перед переговорной – – изолирующие звук и вибрацию обшивки стен 	– устройства вибрационного зашумления
Оптический	<ul style="list-style-type: none"> – окна – двери 	<ul style="list-style-type: none"> – жалюзи на окнах, тонированные или рифленые стекла, доводчики на дверях 	– бликующие устройства
Электромагнитный и электрический	<ul style="list-style-type: none"> – розетки – АРМы – бытовая техника 	<ul style="list-style-type: none"> – сетевые фильтры – генерация шума 	– устройства электромагнитного зашумления

5 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

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

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
4. Все режимные помещения оборудуются аварийным освещением.
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- использование сетевых фильтров;

- установку усиленных дверей;
- дополнительную отделку переговорной комнаты и кабинета директора звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления. В таблице 3 приведён сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 3 – Сравнительный анализ средств активной защиты от утечки виброакустическому каналу

Модель	Диапазон воспроизводимого шумового сигнала	Характеристики	Цена, руб.
ЛГШ-403	180 ÷ 11 300 Гц	ЛГШ-403 обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи на потенциально опасные конструкции помещений. Виброакустические шумовые помехи создаются генератором и передаются на строительные конструкции через вибропреобразователи. Предусмотрена также возможность установки акустического излучателя для защиты закрытых воздушных объемов (воздуховодов, вентиляционных шахт и т.п.). ЛГШ-403 – одноканальный генератор шума.	19 400
ЛГШ-404	175 ÷ 11 200 Гц	Изделие представляет собой генератор шумовых помех и подключаемые к нему по линиям связи пассивные преобразователи – вибровозбудители «ЛВП-10»	35 100

		и акустические излучатели «ЛВП-2а». Генераторный блок оснащен двумя независимыми выходами, к каждому из этих выходов могут быть подключены преобразователи.	
SEL SP-157G	90 ÷ 11.2 кГц	Генераторный блок SEL SP-157G конструктивно содержит два независимых канала генерации с семиполосным (октавным) эквалайзером и двумя параллельными выходами на нагрузку. Каждый канал формирует электрический широкополосный шумовой сигнал маскирующей помехи, состоящий из аналогового белого шума и речеподобной помехи (преобразованной из цифровой).	31 200
ШОРОХ 5Л	175 Гц ÷ 12 кГц	Система «Шорох-5Л» относится к средствам активной акустической и вибрационной защиты информации 1-го класса тип «Б». Система Шорох-5Л состоит из блока питания и управления БПУ-1, конечных вибрационных и акустических излучателей разных типов, размыкателей проводных линий и пульта дистанционного управления. Вибровозбудители закрепляются на оконных рамах, стенах, трубах системы отопления с целью перекрыть виброакустический канал утечки информации. Акустоизлучатели	21 500

		монтируются так, чтобы распространяющиеся от них помехи блокировали акустические каналы похищения данных – воздуховод, вентиляционные трубы, межрамное пространство окон, пр.	
Генератор акустической помехи «Бубен»	400 ÷ 18000 Гц	Используется для защиты конфиденциальных переговоров по принципу создания акустических помех. Вид помех: речеподобная, "белый шум"	15 000 руб.
Система акустических и виброакустических помех «Буран-2»	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.	60 000

В результате анализа был выбран генератор шума Буран. Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать эффективные и

недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники, а также наличием сертификата ФСБ.

5.1 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.

5.2 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 4.

Таблица 4 – Сравнительный анализ средств активной защиты от утечки по электрическому и электромагнитному каналу утечки информации

Модель	Характеристики	Описание	Цена, руб.
Соната РС-3	Напряжение 220 В, частота 50 Гц	После подключения к электросети генерирует электромагнитные шумы – наводки на провода электропитания и заземления. Такие помехи поглощают конфиденциальные данные, содержащиеся в побочных излучениях, и делают невозможным их похищение. Эксплуатационные характеристики: возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения;	32 400

		совместимость с проводными пультами ДУ линейки СОНАТА.	
Соната РС-2	До 2 ГГц	<p>Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ). Также предусмотрена возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus).</p> <p>Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения ("Фаза", "Ноль" и "Защитное заземление") и обеспечивают формирование несинфазных токов и синфазных и парафазных составляющих шумового напряжения во всех проводниках.</p>	23600 руб.
ЛГШ-503	10 кГц – 1,8 ГГц	<p>Изделие «ЛГШ-503» является:</p> <ul style="list-style-type: none"> - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»); - средством активной защиты информации от наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны. 	44 200 руб.


		Изделие «ЛГШ-503» 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.	
ЛГШ-513	0,01–1800 МГц	<p>Изделие «ЛГШ-513» соответствует:</p> <ul style="list-style-type: none"> - типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений; - 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. <p>Изделие «ЛГШ-513» 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.</p>	39 000 руб.
Фильтр сетевой ЛФС-10-1Ф	напряжение 220 В с частотой 50 Гц	Для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от	47 060


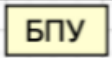
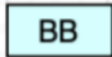

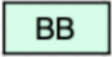

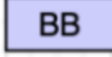

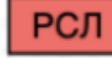
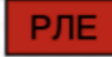


		утечки по каналам побочных электромагнитных наводок. Высокочастотный фильтр, включаемый в сеть напряжением 220 10% В с частотой 50 Гц без соблюдения полярности. Для уменьшения связи между входом и выходом элементы фильтра размещены в трех экранированных отсеках, образованных стенками и шасси изделия.	
Фильтр сетевой ФСПК-10	Напряжение 220В	Сертифицирован ФСТЭК России Устройство защиты речевой информации от утечки по 1- фазным электросетям Количество фильтруемых проводов – 3 Напряжение в электросети – 50 Гц, 220В +/- 10% Максимально допустимая сила тока в сети – 10А Температура эксплуатации – от +1 до +40С	36 300

По результатам сравнительного анализа в качестве средства активной защиты был выбран генератор шума Соната РС-3 из-за ее соотношения цены и качества, этот прибор является эффективным и недорогим, он имеет сертификат ФСТЭК. В качестве пассивной защиты был выбран сетевой фильтр ЛФС-10-1Ф, т.к. он имеет сертификат ФСТЭК и предназначен для работы с государственной тайной.

В таблице 5 представлена смета.

Таблица 5 – Смета

Наименование	Кол-во, шт.	Цена за единицу, руб.	Стоимость, руб	Обозначение
Рулонные жалюзи Blackout	6	1 773	10 638	

Усиленные звукоизолирующие двери Ultimatum PP	5	75 283	376 415	
Виброакустический генератор «Буран-2»	1	45 000	45 000	
Вибропреобразователь для стен «Молот» с креплением	18	3 000	54 000	
Вибропреобразователь для коммуникаций «Серп-Т» с креплением	8	3 000	24 000	
Вибропреобразователь для рам «Серп-Р» с креплением	6	3 000	18 000	
Вибропреобразователь для окон «Копейка» с креплением на раму окна	6	2 500	15 000	
Преобразователь акустический «Рупор»	4	2 000	8 000	
Модуль дистанционного управления по проводному каналу «Буран-ДУ»	1	4 500	4 500	
Размыкатель линий оповещения и сигнализации «Буран-К2»	1	3 400	3 400	
Размыкатель компьютерных сетей «Буран-К3»	2	3 500	7 000	
Соната РС-3	4	32 400	129 600	
ЛФС-10-1Ф	1	47 060	47 600	

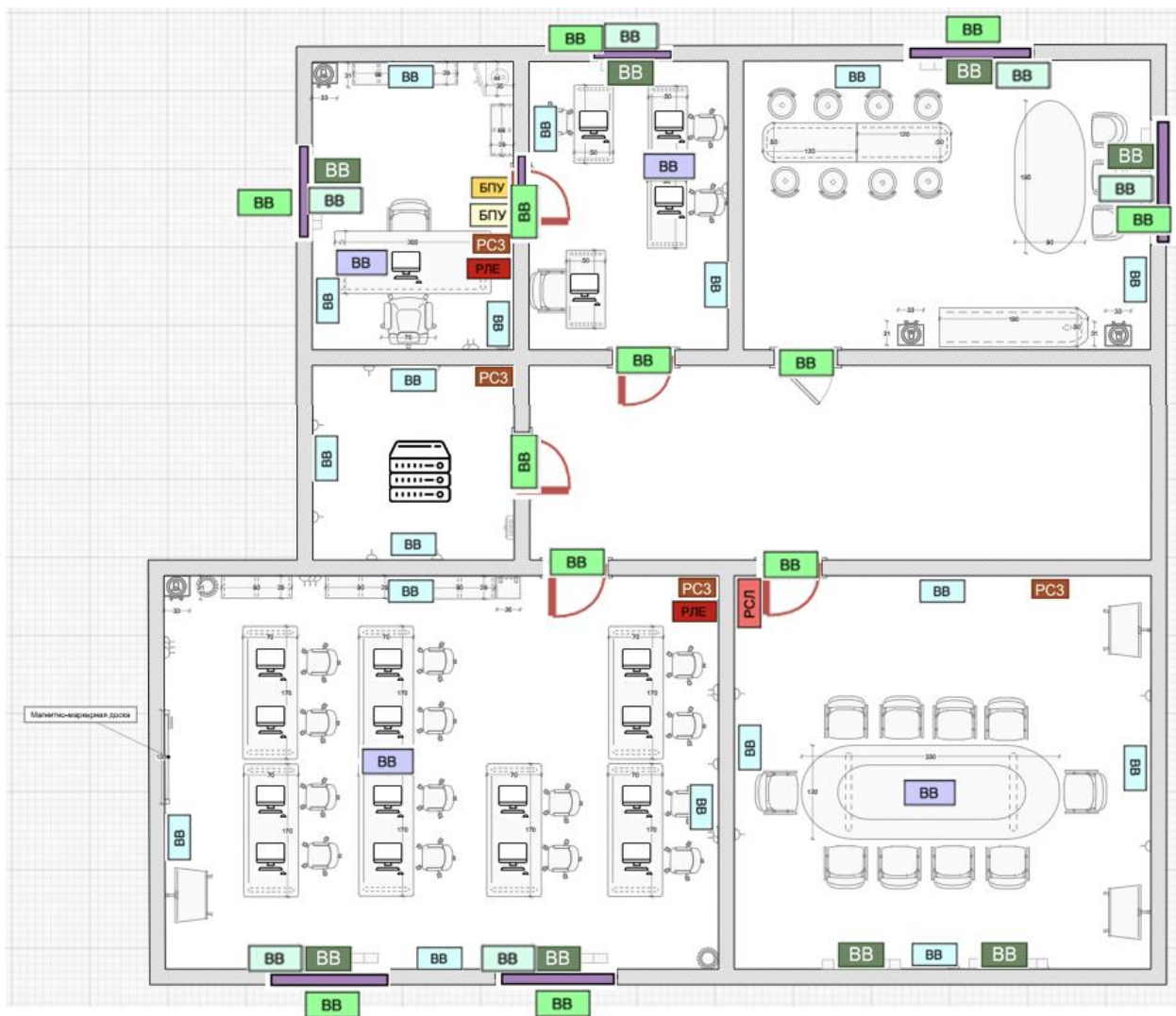


Рисунок 4 – Размещение средств защиты

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы были изучены активные и пассивные методы защиты, проведена классификация технических каналов утечки информации, проведён 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.

ИСТОЧНИКИ

1. Утечки данных в России// Tadviser — URL: tadviser.ru/index.php/Статья:Утечки_данных_в_России (дата обращения: 25.11.2023).
2. Утечки информации ограниченного доступа в мире 2022 г. // InfoWatch — URL: <https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g> (дата обращения: 01.12.2023).
3. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи // Спецтехника. — 2018. — № 2. — С. 17-22.
4. Соколов, А. И. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие /А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2006 – 71 с. (Комплексная защита объектов информатизации. Кн. 13 / под ред. М. Ю. Монахова).
5. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения – URL: <https://docs.cntd.ru/document/1200075565> (дата обращения: 27.11.2023).
6. Виброакустический канал утечки информации // SearchInform — URL: <https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/vibroakusticheskij-kanal-utechki-informatsii/> (дата обращения: 30.11.2023).
7. Хорев А. А. Способы защиты объектов информатизации от утечки информации по техническим каналам: защита цепей электропитания средств вычислительной техники // Спецтехника. — 2013. — № 1. — С. 30-37.