

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

Факультет безопасности информационных технологий

КУРСОВОЙ ПРОЕКТ

по дисциплине:

«Инженерно-технические средства защиты информации»

на тему:

Проектирование системы защиты от утечки информации по различным каналам

Выполнила:

студент группы N34521

Прохиرو Дарья

Александровна

_____  _____

Проверил:

Попов И. Ю.

Оценка: _____

Подпись: _____

«__» _____ 2023 г.

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Прохира Дарья Александровна

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34521

Направление (специальность) Комплексные системы защиты информации

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

Задание Разработка комплекса инженерно-технической защиты информации в помещении

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 _____

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Прохира Дарья Александровна

(Подпись, дата)


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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА (РАБОТЫ)

Студент Прохиро Дарья Александровна
(Фамилия И.О.)
Факультет Безопасности Информационных Технологий
Группа N34521
Направление (специальность) Комплексные системы защиты информации
Руководитель Попов Илья Юрьевич, к. т. н., доцент ФБИТ
(Фамилия И.О., должность, ученое звание, степень)
Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	16.09.2023	16.09.2023	
2	Анализ теоретической составляющей	11.11.2023	11.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.2023	20.11.2023	
4	Представление выполненной курсовой работы	05.12.2023	05.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата) 
Студент Прохиро Дарья Александровна
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВОЙ ПРОЕКТ (РАБОТУ)

Студент Прохиро Дарья Александровна

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34521

Направление (специальность) Комплексные системы защиты информации

Руководитель Попов Илья Юрьевич, к. т. н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

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

☐ 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 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)



Студент Прохиро Дарья Александровна

(Подпись)

«__» _____ 20__ г.

Оглавление

Введение.....	6
1 Анализ технических каналов утечки информации.....	7
2 Руководящие документы.....	13
3 Анализ защищаемых помещений.....	17
4 Анализ технических средств защиты информации.....	23
5 Описание расстановки технических средств	29
Заключение	31
Список используемой литературы	32

Введение

В современном мире на каждом предприятии существует информация, которую необходимо защищать различными методами и средствами от нежелательных пользователей таких, как конкурирующие предприятия, мошенники, шпионы и т.д. Попад в чужие руки, ценная информация становится товаром. Ее искажение, порча или плагиат могут навредить репутации и финансам компании. Именно сохранение в тайне конфиденциальной информации дает возможность предприятию успешно выводить на рынок технологические новинки и быть конкурентоспособным.

В данной курсовой работе будут рассмотрены способы защиты от утечки информации по техническим каналам с помощью инженерно-технических средств защиты информации.

Инженерно-технические средства защиты информации — это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации. Защита при помощи данных средства необходима так, как сейчас активно развиваются различные средства добычи информации, которые позволяют получать несанкционированный доступ к данным на расстоянии. В тоже время стало доступно для любого пользователя использование радио и электроаппаратуры, аудио жучков, мини камер и других устройств, что также дает возможность получить незаконным способом доступ к защищаемой информации. Использование надежных технических средств защиты информации становится единственным способом предотвратить возможную утечку данных.

Данная курсовая работа состоит из пяти частей. В первой части будет проведен анализ технических каналов утечки информации, во второй части будут приведены руководящие документы, в третьей части — анализ помещения и возможные каналы утечки информации. Последние две части представляют собой анализ технических средств и их расстановка в помещении.

1 Анализ технических каналов утечки информации

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Технический канал утечки информации (ТКУИ) – это совокупность источника информации, линий связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линиях связи, и технических и программных средств перехвата информации.

Утечка информации по техническому каналу – это неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

На рисунке 1 представлена схема структуры ТКУИ.

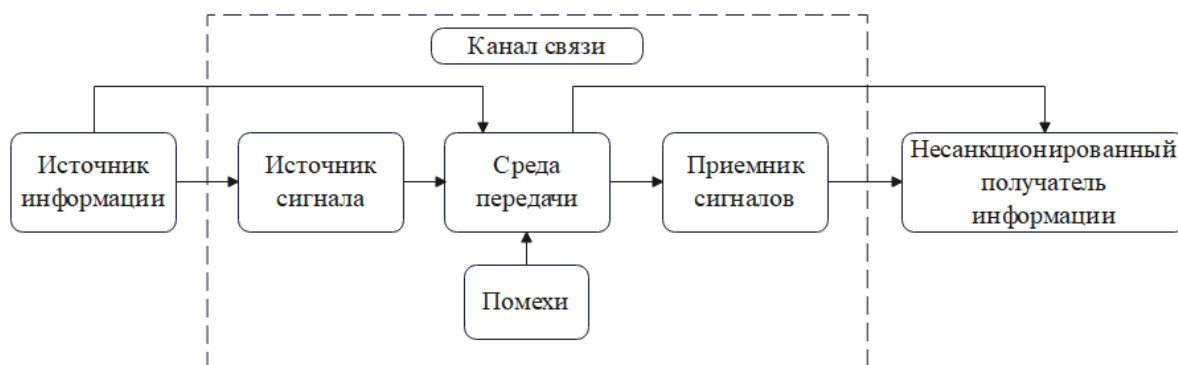


Рисунок 1. Структура технического канала утечки информации

Технический канал содержит три основных элемента: источник сигнала, среду распространения носителя и приемник. 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.

В образовании канала утечки участвуют разнообразные вспомогательные технические средства и системы (ВТСС), которые не используются непосредственно при обработке информации. Они способны излучать электромагнитные и световые волны, распространять звуковые сигналы, изменять физические параметры из-за соседства с основной техникой.

К ВТСС относятся линии электропитания и связи, выходящие за границы контролируемой зоны, а также климатическое оборудование, металлические трубы отопления, водоснабжения и канализации.

Похищение секретных сведений осуществляется путем улавливания излучений от основной и вспомогательной аппаратуры, подключения специальных закладных устройств к каналам связи, исследования объектов информации, выходящих за пределы защищаемой зоны.

Технический канал утечки позволяет злоумышленникам перехватывать информационные сигналы различной природы, получая несанкционированный доступ к конфиденциальным сведениям. В составе ТКУИ имеются источник сигнала (интересующий объект, обладающий определенными физическими, химическими, биологическими свойствами), среда распространения (воздушная, безвоздушная, жидкая, твердая) и перехватчик сигнала (технические средства приема данных (ТСПИ) или объект, заинтересованный в похищении ценной информации).

К ТСПИ относятся:

- Электронная оргтехника (компьютеры, принтеры, копировальные устройства);
- Аппаратура автоматизированных систем управления (АСУ);
- Вычислительные машины;
- Акустическая аппаратура (микрофоны, усилители звука, устройства звуковоспроизведения и синхронного перевода);
- Оптические приборы (фотоаппаратура, электронные микроскопы);
- Аппаратура внутренней связи;
- Видеоустройства, сигнальное и охранное оборудование;
- Внутренние проводные линии связи.

В зависимости от вида используемых и технических средств передачи информации (ТСПИ) и природы сигнала ТКУИ подразделяются на группы, представленные на рисунке 2.

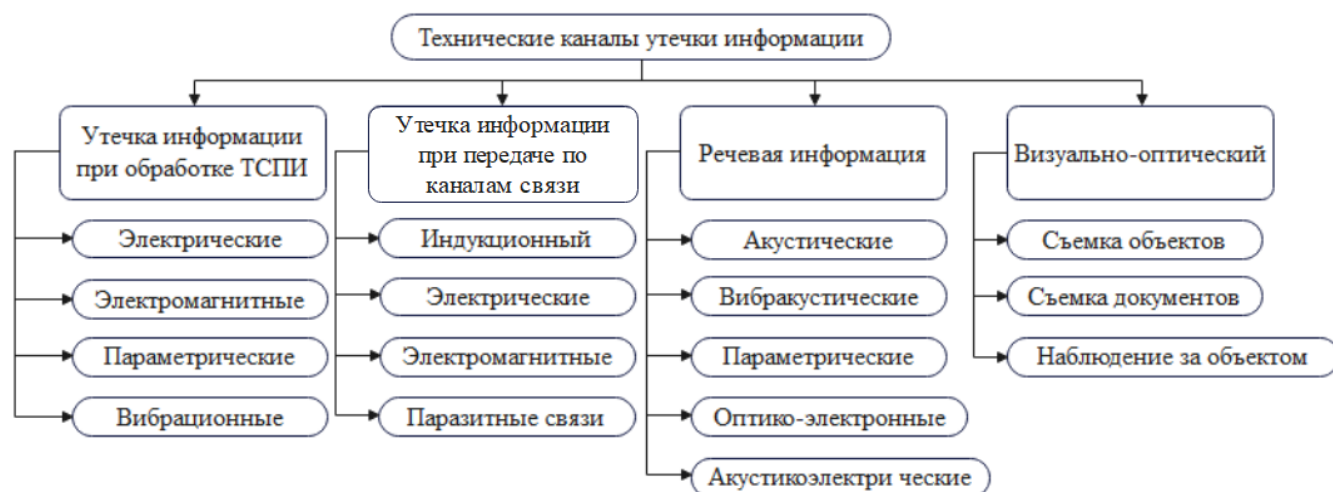


Рисунок 2. Виды ТКУИ

1. Технические каналы утечки информации при обработке техническими средствами передачи информации.

При выявлении технических каналов ТСПИ необходимо рассматривать совокупность

основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС).

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ).

Контролируемая зона – территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические, параметрические и вибрационные.

1) Электрические каналы

Электрические каналы утечки информации возникают за счёт:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы КЗ. Возникают при излучении элементами ТСПИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС;
- просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ. Возможно, при наличии магнитных связей между выходным трансформатором усилителя (например, УНЧ) и трансформатором блока питания;
- использования закладных устройств.

2) Электромагнитные каналы

К электромагнитным относятся каналы утечки информации, возникающие за счёт различного вида побочных электромагнитных излучений и наводок (ПЭМИН) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ. В результате внешних воздействий информационного сигнала на элементах ВЧ – генераторов наводятся электрические сигналы, которые могут вызвать паразитную модуляцию собственных ВЧ – колебаний генераторов.;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ. Самовозбуждение УНЧ ТСПИ возможно за счёт образования случайных паразитных обратных связей, что приводит к переводу усилителя в режим автогенерации сигналов.

3) Параметрические каналы

Перехват информации возможен путём «высокочастотного облучения» («электромагнитного навязывания») ТСПИ. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля.

В ряде случаев это вторичное излучение имеет модуляцию, обусловленную воздействием информационного сигнала. Для перехвата информации по параметрическому каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные приёмные устройства.

4) Вибрационные каналы

Некоторые ТСПИ имеют в своём составе печатающие устройства, для которых можно найти соответствие между распечатываемым символом и его акустическим образом. Данный принцип лежит в основе канала утечки информации по вибрационному каналу.

2. Каналы утечки информации при её передаче по каналам связи

Для передачи информации используются КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, различные виды телефонной радиосвязи (сотовые, транкинговые, Dect, Wi-Fi и др.), а также кабельные и волокно–оптические линии связи.

В зависимости от вида канала связи технические каналы перехвата (утечки) информации можно разделить на электромагнитные, электрические, индукционные и паразитные связи.

1) Электромагнитные каналы

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки. Данный канал утечки наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым средствам связи и радиорелейным и спутниковым линиям связи.

2) Электрические каналы

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи. Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи (через согласующие устройства). Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, для предотвращения срабатывания специальной сигнализации.

3) Индукционный канал

В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики применяются в основном для съёма информации с симметричных высокочастотных кабелей.

4) Паразитные связи

В результате воздействия побочных полей и влияния через проводники и резисторы сигналов одних узлов и блоков на сигналы других блоков и узлов возникают паразитные связи

3. Технические каналы утечки речевой информации

Под воздействием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своём первоначальном виде речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. В зависимости от среды распространения речевых сигналов и способов их перехвата технические каналы утечки речевой информации можно разделить на: акустические, вибрационные, акустоэлектрические, оптоэлектронные и параметрические.

1) Акустические каналы

В акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные и направленные микрофоны, соединённые с портативными записывающими устройствами или со специальными передатчиками.

2) Виброакустические каналы

В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений и инженерные коммуникации. Для перехвата речевых сигналов в этом случае используют вибродатчики (акселерометры).

3) Параметрические каналы

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала.

Параметрический канал утечки информации может быть организован и путём «высокочастотного облучения» помещения, где установлены закладные устройства, имеющие элементы, параметры которых изменяются под действием акустического (речевого) сигнала.

4) Оптико – электронный канал

Оптико – электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стёкол, зеркал и т.д.). Отражённое лазерное излучение модулируется по амплитуде и фазе и принимается приёмником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация

5) Акустоэлектрические каналы

Акустоэлектрические каналы утечки информации возникают за счёт преобразований акустических каналов в электрические. Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных часов, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (ёмкость, индуктивность, сопротивление) под

действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающим по этим элементам в соответствии с изменениями воздействующего электрического поля.

4. Визуально-оптический канал утечки информации

В зависимости от характера информации можно классифицировать следующие способы получения ее изображений: наблюдение за объектами, съёмка объектов, снятие копии документов.

1) Наблюдение за объектами

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства. Для наблюдения днём – оптические приборы, телевизионные камеры, для наблюдения ночью – приборы ночного видения, телевизионные камеры, тепловизоры. Для наблюдения с большого расстояния используются средства аэро – и космической кино – фотосъёмки, длиннофокусные оптические системы, а для наблюдения с близкого расстояния – камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

2) Съёмка объектов

Съёмка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съёмки объектов используются телевизионные и фотографические средства, включая аэро – космические.

3) Съёмка документов

Съёмка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

2 Руководящие документы

Перечень основных руководящих документов в области информационной безопасности.

Федеральное законодательство:

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
2. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
4. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
5. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
6. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры»;
7. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1;
8. Федеральный закон от 20.02.1995 N 24-ФЗ (ред. от 10.01.2003) "Об информации, информатизации и защите информации".

Указы президента РФ:

1. Указ Президента РФ № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
2. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
3. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
4. Указ Президента Российской Федерации от 30.03.1994 № 614 «Вопросы защиты государственной тайны»;
5. Указ Президента РФ от 6 октября 2004 г. N 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»;
6. Указ Президента Российской Федерации от 08.11.1995 № 1108 «О Межведомственной комиссии по защите государственной тайны»;
7. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

Постановления Правительства РФ:

1. Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных»;
2. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О

сертификации средств защиты информации»;

3. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
4. Постановление Совета Министров — Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»;
5. Постановление Правительства РФ от 15 апреля 1995 г. N 333 "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";
6. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
7. Постановление Правительства РФ от 6 февраля 2010 г. N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

Руководящие документы по защите информации от НСД. (Гостехкомиссия):

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение Гостехкомиссии России от 30.03.1992
2. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение Гостехкомиссии России от 30.03.1992
3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение Гостехкомиссии России от 30.03.1992
4. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение Гостехкомиссии России от 30.03.1992
5. 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. Решение Гостехкомиссии России от 30.03.1992

6. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России 1997г
7. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссии России 1997 г.

Нормативно-технические документы ФСТЭК России:

1. СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
2. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;
3. Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;
4. Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
5. Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
6. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения
7. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
8. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации
9. 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
10. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации
11. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования

12. Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей
13. Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам

Другие нормативно-правовые документы в области защиты информации:

1. Межведомственная комиссия по защите государственной тайны решения № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

3 Анализ защищаемых помещений

Наименование организации: ООО «CliningLab»

Область деятельности: клиническая диагностика

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

Основные информационные процессы:

1. Предоставление информации об услугах
2. Сбор заявок на исследования и необходимого информационного сопровождения
3. Предоставление пользователям инструментов для заказа услуги и создания учётной записи на сайте
4. Доступ к результатам исследований клиенту
5. Ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией
6. Хранение, обработка, передача, утилизация персональных данных пользователей
7. Хранение данных о биоматериале, сданном клиентами
8. Хранение данных о внутренних биотехнологических разработках
9. Формирование необходимой отчетной и иной статистической документации
10. Усовершенствование способов исследований

Основные информационные потоки:

1. Открытые потоки: взаимодействие с отделом по работе с клиентами (служба поддержки, отдел по работе с ключевыми клиентами, отдел предоставления услуг), взаимодействие с маркетинговым отделом, взаимодействие с отделом контроля качества.
2. Закрытые потоки: взаимодействие с отделом клинических исследований, взаимодействие с отделом закупок, взаимодействие с отделом безопасности, взаимодействие с отделом ИТ, взаимодействие с маркетинговым отделом (направление развития), взаимодействие с бухгалтерией, взаимодействие с отделом по работе с клиентами (финансы).

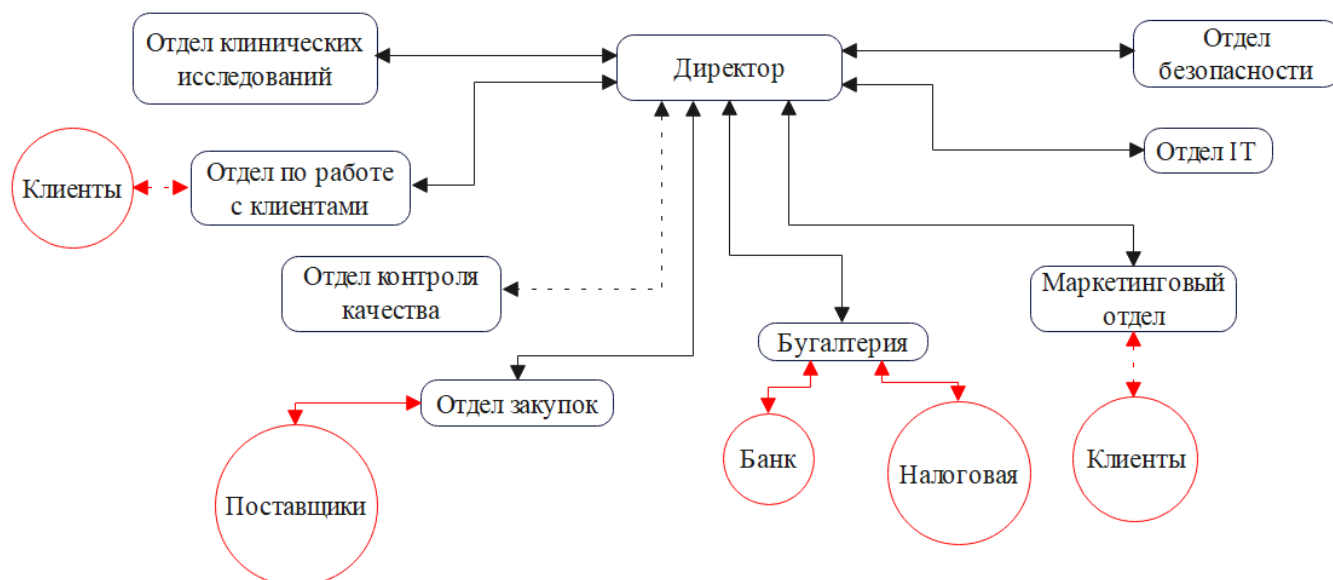


Рисунок 3. Информационные потоки

Информация ограниченного доступа:

1. Персональные данные сотрудников – информационный актив, хранящийся в электронной форме, владельцами являются руководители отделов, отдел безопасности.
2. Персональные данные клиентов – информационный актив, хранящийся в электронной форме, владельцами являются отдел клинических исследований, отдел по работе с клиентами и отдел безопасности.
3. Коммерческая тайна – информационный актив, хранящийся в электронной форме, владельцем является компания.
4. Биоматериал клиента – информационный актив, хранящийся в электронной форме, владельцем является отдел клинических исследований.
5. Результаты исследований – информационный актив, хранящийся в электронной форме, владельцем является отдел клинических исследований.
6. Техническая информация (пароли, логины, расположение элементов сети и т.д.) – информационный актив, хранящийся в электронной форме, владельцами являются отдел ИТ, отдел безопасности.

Система имеет классификацию «Секретно». Компания работает со сведениями, составляющие государственную тайну. Государственной тайной является информация о новых разработках в медицине, а также информация, полученная от заказчика, в роли которой выступают государственные структуры. Система имеет 3 тип формы доступа для граждан, допускаемых к секретным сведениям.

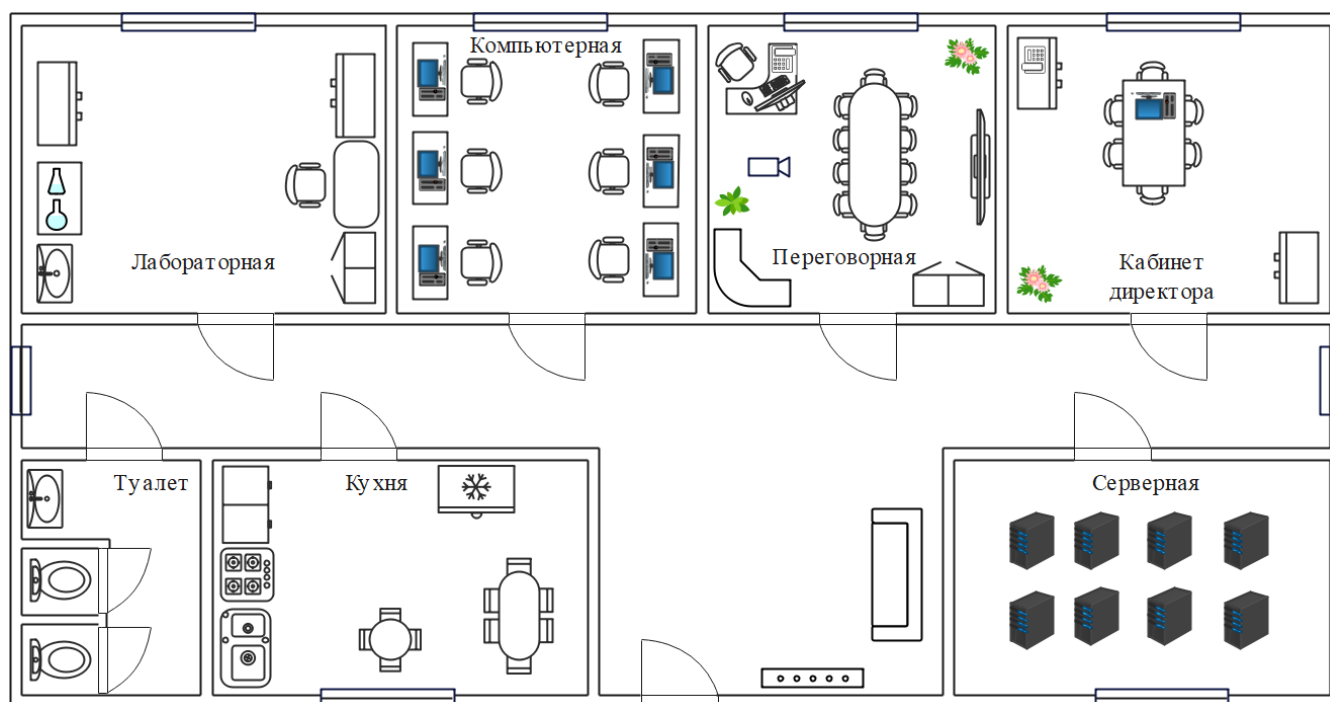



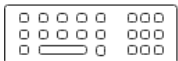





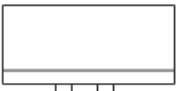
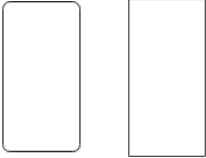


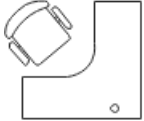
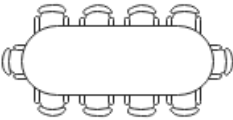
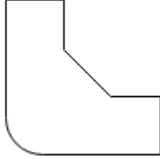
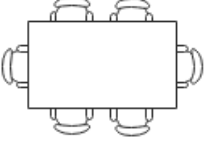
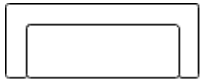




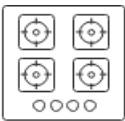

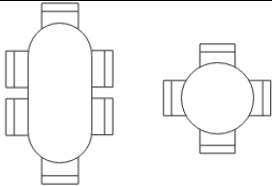


Рисунок 4. План помещения

Обозначения	Описание
	Персональный компьютер
	Монитор
	Компьютерная мышка
	Клавиатура
	Стационарный телефон
	Экран для проектора
	Игровая приставка
	Колбы
	Сервер
	Шкаф

	Столы
	Шкаф для вещей
	Стул
	Стол со стулом
	Стол для переговоров
	Книжный стеллаж
	Стол директора
	Диван
	Вешалка для верхней одежды
	Живые растения
	Раковины

	Унитаз
	Кухонная плита
	Холодильник
	Кухонные столы

Защите подлежат следующие помещения:

- Кабинет директора: 6.1 м на 6.6 м, площадь 40.26 м²
- Переговорная: 6.1 м на 5.9 м, площадь 35.99 м²
- Серверная: 5.8 м на 7 м, площадь 40.6 м²
- Компьютерная: 6.1 м на 6.4 м, площадь 39.04 м²
- Лабораторная: 6.1 м на 7.8 м, площадь 47.58 м

Помещение состоит из 7 комнат и коридора. Необходимо защищать 5 комнат, содержащих информацию ограниченного доступа. Переговоры введутся в кабинете директора и переговорной. В кабинете директора находятся стол со стульями, 2 шкафа, персональный компьютер, телефон, живое растение, батарея центрального отопления, 3 розетки, 1 окно. В переговорной находится стол со стульями, книжный шкаф открытый, шкаф для вещей, стол, стул, персональный компьютер, телефон, проектор, экран для проектора, 2 живых растения, 4 розетки, батарея центрального отопления, окно. В серверной располагаются стеллажи с серверами, 16 розеток, окно. В компьютерной располагаются 6 столов, 6 стульев, 6 персональных компьютеров, 12 розеток, батарея центрального отопления, окно. В лабораторной располагается 2 шкафа с веществами, шкаф для вещей, 2 стола, стул, раковина, колбы, 4 розетки, батарея центрального отопления, окно.

Помещение расположено на втором этаже пятиэтажного здания. Здание располагается на охраняемой территории отдельно от остальных. Окна располагаются вдали от пожарных и эвакуационных лестниц. Около окон нет пристроек, выступов, балконов и других элементов, при помощи которых посторонние лица могли бы проникнуть в помещение.

В помещении располагаются декоративные элементы, в которые могут быть подложены

закладные устройства. Также существует возможность утечки информации с помощью электрического и электромагнитного каналов, так как в каждом кабинете имеются розетки. Имеется угроза снятия информации по вибрационному, оптическому каналам, акустическому, виброакустическому и акустоэлектрическому.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации и относится к организационно-правовой защите информации.

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

4 Анализ технических средств защиты информации

Организация работает с информацией, относящейся к государственной тайне уровня «секретно». Согласно решению Межведомственной комиссии по защите государственной тайны № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними" введены следующие требования к оборудованию в режимных помещениях, содержащих государственную тайну:

1. Стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см.
2. В помещениях для работы с гостайной 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.
3. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
4. 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.
5. Все режимные помещения оборудуются аварийным освещением.
6. Что касается оборудование помещений для работы с гостайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений. 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 электрического, акустоэлектрического и электромагнитного каналов утечки информации

Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала. Для пассивной защиты от электрического, акустоэлектрического и электромагнитного

каналов утечки информации необходимо установить фильтры для сетей электропитания во всех помещениях.

Цель активного способа защиты – обеспечить создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Для активной защиты от электрического, акустоэлектрического и электромагнитного каналов утечки информации необходимо создать в сети белый шум, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой.

Таблица 2. Сравнительный анализ средств защиты

Устройство	Характеристики	Предназначение	Цена, рублей
Генератор шума ЛГШ-503	Диапазон частот 10 кГц - 1800 МГц; Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц); Мощность 45 Вт Наработка на отказ 12000 часов	Защиты информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.	44 200
SEL-155 «СОНЕТ»	Диапазон частот от 0,01 до 1800 МГц; Уровень шума до 32 дБ; Мощность 30 Вт для управляющего блока	Система предназначена для защиты телефонных линий, линий компьютерных сетей, соединительных линий систем оповещения и сигнализации от утечки по каналу акустоэлектрических преобразований.	22 000
ГАММА ГШ-18	Диапазон частот от 0,01 до 1800 МГц; Уровень шума уровень сигнала на нагрузке 50 Ом во всем диапазоне частот не менее 50 дБ/мкВ, диапазон регулировки выходного сигнала от 0 до 20 дБ; Мощность 50 дБ/мкВ; Наработка на отказ 20000 ч	Предназначен для маскировки ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей и комплексов на объектах вычислительной техники второй, третьей и четвертой категорий, путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) и наведения шумового сигнала на токопроводящие линии и инженерно-технические коммуникации, включая цепи электропитания и заземления, в широком диапазоне частот.	29 400
Генератор шума ГНОМ-3М	Диапазон частот 0,15 до 1800МГц; Уровень шума 25 - 75 дБ/мкВ; Мощность 40Вт	Предназначен для активной защиты информации, обрабатываемой на электронно-вычислительной технике.	57 200
Фильтр сетевой	Диапазон частот 0,15-	Предназначен для защиты	33 264

помехоподавляющий ФСП-1Ф-7А	1000 МГц; Вносимое затухание по напряжению в каждом проводе двухпроводной сети не менее 60 дБ; Допустимый ток нагрузки 7 А	радиоэлектронных устройств и средств вычислительной техники от утечки информации по цепям электропитания с напряжением 220В с током нагрузки до 7А.	
Фильтр сетевой помехоподавляющий ФПБМ-3	Ток 20 А; Частотный диапазон от 0,01 до 10000 МГц; Затухание 60 до 90Дб	Предназначен для защиты от утечки или специально организованной передачи информации по цепям питания 220 (380)В / 50Гц с током нагрузки до 20А.	30 960
Фильтр сетевой помехоподавляющий ФПБД	Ток 15 А; Частотный диапазон от 0,01 до 1000 МГц; Затухание 30 до 60Дб	Предназначен для защиты информации на различных устройствах типа вычислительной техники и прочих радиоэлектронных устройствах, где возможна утечка посредством наводок по электрическим цепям.	15 840
Фильтр сетевой помехоподавляющий ФСШК-2	Ток 6 А; Частотный диапазон от 0,01 до 1000 МГц; Затухание 40 до 70Дб	Предназначен для защиты информации на различных устройствах типа вычислительной техники и прочих радиоэлектронных устройствах, где возможна утечка посредством наводок по электрическим цепям.	13 824

В результате анализа был выбран генератор шума ГАММА ГШ-18. В генераторе предусмотрена плавная регулировка уровня выходного сигнала, также достаточно широкий диапазон и не дорогая стоимость. Для пассивной защиты предлагается выбрать фильтр сетевой помехоподавляющий ФПБД.

Защита от ПЭМИН

Для реализации активной защиты от ПЭМИН было также выбрано устройство ГАММА ГШ-18.

Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- усиленные двери,
- тамбурное помещение перед переговорной,
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического шумления. Для защиты помещения для работы с государственной тайной уровня «совершенно секретно» рассматриваются технические средства активной защиты информации для объектов

информатизации категории не ниже 1Б.

Таблица 3. Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, рублей
Генераторный блок "ЛГШ-404"	Диапазон частот 175-11200 Гц; Количество подключаемых излучателей на канал до 20 шт; Мощность, потребляемая от сети не менее 25 ВА	Предназначено для защиты акустической речевой информации от утечки по виброакустическому и акустическому каналам. Изделие соответствует типу «А» – средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными преобразователями.	35 100
Бубен-Ультра Макс	Частота приемника/передатчика РПДУ 433 МГц; Количество ультразвуковых излучателей, до 48 шт.	Предназначен для подавления звукового сигнала при попытке записи на записывающие устройства, специальные технические средства, выносные микрофоны посредством генерации трех типов помех.	50 400
SEL SP-157G - генератор акустических и виброакустических помех системы SEL-157 "ШАГРЕНЬ".	Частоты 250, 500, 1000, 2000, 4000 и 8000 Гц; Диапазон регулировки общего интегрального уровня шумового сигнала 30Дб	Содержит два независимых канала генерации с семи полосным (октавный) 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
Система акустических и виброакустических помех Буран	Диапазон частота 100 – 11 200 Гц Диапазон регулировки общего интегрального уровня шумового сигнала 30Дб; Максимальное число изделий, объединяемое в одну группу для их группового подключения к сети электропитания 20 шт.	Средство активной акустической и вибрационной защиты акустической речевой информации типа А, соответствует требованиям ФСТЭК России к средствам защиты акустической речевой информации по 2 классу защиты и может устанавливаться в выделенных помещениях.	67 500
Система акустических и виброакустических помех Буран-2	Диапазон рабочих частот не менее 180-11200 Гц; Мощность, потребляемая от сети не более 20 Вт	Средство активной акустической и вибрационной защиты акустической речевой информации, может использоваться для защиты акустической речевой информации, содержащей сведения, составляющие государственную	81 000

		тайну, циркулирующей в выделенных помещениях до 2 категории включительно.	
"ANG-2200" - генератор шума	Диапазон акустического шума 250 Гц - 5 кГц; Кол-во ультразвуковых излучателей до 18 шт.	Для защиты помещений от возможного прослушивания через проводные микрофоны, радиомикрофоны и стетоскопы, блокирования лазерного съема акустической информации с окон, создания помех звукозаписывающей аппаратуре.	18 000
Акустический подавитель диктофонов Троян-2	Уровень звукового давления 80 дБ; Напряжение сигнала помехи на линейном выходе 0,25 В	Для подавления всех существующих диктофонов, в т.ч. в сотовых телефонах, любых радиомикрофонов, предотвращение съема акустической информации со стекол, стен и других инженерных конструкций здания.	24 900
Соната-АВ модель 4Б	Диапазон воспроизводимого шумового сигнала 175 – 11200 Гц; Максимальное количество излучателей 239 шт.	Генератор шума. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы.	44 200
Канонир-К7	Уровень звукового давления 100 дБ / 95 - 100 дБ; Дальность подавления диктофонов, до 2 - 4 м	Использует сразу 2 способа защиты от прослушки. Подавление происходит с помощью генерации звуковой речеподобной помехи и ультразвука.	37 000
ULTRASONIC-SPYLINE-24-LIGHT	Уровень звукового давления 90 дБ; Кол-во излучателей 24; Дальность подавления диктофонов, до 1.5 - 5 м	Виброакустические излучатели мешают проникновению лазерных микрофонов и сбору информации с оконных стекол переговорных залов, тем самым обеспечивая вам надежную защиту и конфиденциальность.	37 981
Подавитель Тайфун-5Б	Уровень звукового давления до 110 дБ; Дальность подавления диктофонов, до 3 метров	Подавление диктофонов в сотовых телефонах, в смартфонах типа iPhone, в планшетных компьютерах типа iPad.	62 479
SEL-310 «КОМАР»	Диапазон частот УЗ помехи 24 - 26 кГц; Кол-во излучателей 10 шт; Дальность подавления диктофонов, до 4 м	Предназначен для полного подавления полезного звукового сигнала при попытке записи.	60 000
Соната ИП-4.1	Нагрузочная способность не менее 1500 мА Мощность, потребляемая от сети не более 40 Вт	Составная часть системы виброакустической защиты для выделенных помещений и защиты от прослушивания кабинетов первых лиц и переговорных комнат	26 400

По результатам анализа была выбрана система генераторный блок "ЛГШ-404". Конструкция изделия обеспечивает защиту органов регулировки выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним

Также был выбран подавитель микрофонов Бубен-Ультра Макс. Он генерирует три типа помех: помехи в ультразвуковом диапазоне, воздействующей непосредственно на мембрану микрофона; сложные звуковые помехи, воздействующей на АРУ записывающего устройства, тем самым увеличивая воздействие УЗП; речеподобные помехи с периодической перестройкой во времени, для затруднения ее выделения из полезного сигнала. Также есть защита от выхода из строя из-за повышенного и пониженного напряжения источника питания.

Защита от утечек по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, наиболее комфортным и недорогостоящим будет установка на окно жалюзи или шторы. С точки зрения удобства содержания были выбраны жалюзи.




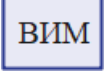


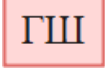



5 Описание расстановки технических средств


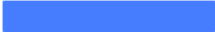

Согласно информации, приведённой в 4 главе, выбранные средства защиты информации включают в себя:

- Генераторный блок "ЛГШ-404";
- Бубен-УльтраМакс;
- Генератор шума ГАММА ГШ-18;
- Фильтр сетевой помехоподавляющий ФПБД
- Жалюзи на окна в количестве 5 штук;
- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей

прокладкой на металлическом каркасе – 2 шт., в переговорную и архив.

Таблица 4. Смета

Мера защиты	Обозначение	Цена, руб.	Количество, шт.	Стоимость, руб.
Блок питания и управления "Гамма-01 БПУ"		54 000	1	54 000
Вибрационный излучатель «Серп-Р» (стены, пол)		3 000	32	96 000
Вибрационный излучатель «Серп» (двери)		3 000	8	24 000
Вибрационный излучатель «Молото» (окна)		3 000	8	24 000
Подавитель диктофонов Бубен-Ультра Макс		50 400	1	50 400
Генераторный блок "ЛГШ-404"		35 100	1	35 100
Генератор шума ГАММА ГШ-18		29 400	5	147 000
Фильтр сетевой помехоподавляющий ФПБД		15 840	1	15 840
Размыкатель Телефонной линии "Соната-ВК4.1"		6 000	1	6 000
Размыкатель Слаботочной линии "Соната-ВК4.2"		6 000	1	6 000

Размыкатель линии Ethernet "Соната-ВК4.3"		6 000	1	6 000
Рулонные шторы РИКАМО светонепроницаемая 52*170 см		1 117	5	5 585
Усиленные металлические двери Б-29		23 000	5	115 000
Итого				584 925

Результаты расстановки средств защиты информации от утечки по техническим каналам представлены на рисунке 5.

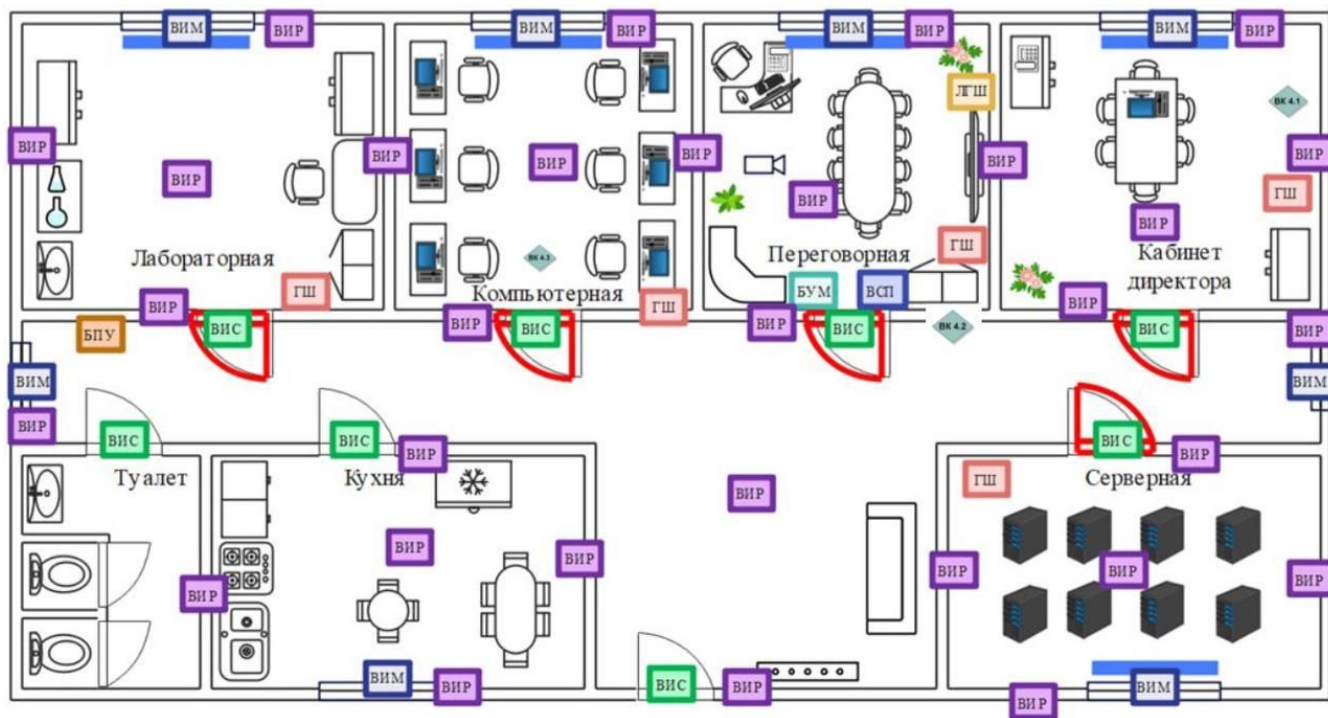


Рисунок 5. Схема расстановки устройств

Заключение

В ходе курсовой работы были проанализированы существующие технические каналы утечки информации, возможные технические каналы утечки информации для защищаемого помещения организации ООО «CliningLab», которая работает с государственной тайной уровня «секретно». По результатам анализа помещения был проанализирован рынок существующих средств для противодействия рассматриваемым каналам утечки информации и выбраны необходимые средства для защищаемого помещения. Также был разработан план установки данных средств и подсчитаны затраты на закупку данных средств.

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

Список используемой литературы

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: 19.12.2022).
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: 17.12.2022)