

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

**Факультет безопасности информационных технологий**

**КУРСОВАЯ РАБОТА**

**По дисциплине:**

**«Инженерно-технические средства защиты информации»**

**На тему:**

**«Проектирование инженерно-технической системы защиты информации на  
предприятии. Вариант 57»**

**Выполнил(а):**

Студент группы N34481

Узаков Айдар

Нурланович



**Проверил преподаватель:**

Попов Илья Юрьевич,

доцент ФБИТ, к. т. н.

**Отметка о выполнении:**

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	Узаков Айдар Нурланович
	(Фамилия И.О.)
Факультет	Безопасности Информационной Технологий
Группа	N34481
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	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 57
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**

**Рекомендуемая литература**

Руководитель

Студент



(Подпись, дата)

25 октября 2023

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент**      Узаков Айдар Нурланович  
\_\_\_\_\_  
(Фамилия И.О.)

**Факультет**      Безопасности Информационных Технологий  
\_\_\_\_\_

**Группа**      N34481  
\_\_\_\_\_

**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**      Проектирование инженерно-технической системы защиты информации  
на предприятии. Вариант 57  
\_\_\_\_\_

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	16.09.23	16.09.23	
2	Анализ теоретической составляющей	11.11.23	11.11.23	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.23	20.11.23	
4	Представление выполненной курсовой работы	19.12.23	19.12.23	

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

**Студент**       19 декабря 2023  
\_\_\_\_\_  
(Подпись, дата)

Студент	Узаков Айдар Нурланович
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34481
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	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 57

1. Цель и задачи работы

☐ Предложены студентом      ☐ Сформулированы при участии студента


☒ Определены руководителем

2. Характер работы

<input type="checkbox"/> Расчет	<input type="checkbox"/> Конструирование
<input type="checkbox"/> Моделирование	<input checked="" type="checkbox"/> Другое

В работе представлены результаты анализа технических каналов утечки информации, требований к защите помещений с различным уровнем секретности, а также рынка инженерно-технических средств защиты информации. На основе результатов анализа разработана инженерно-техническая система защиты информации.

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

Студент  28 октября 2023

## СОДЕРЖАНИЕ

Введение .....	6
1     Анализ технических каналов утечки информации .....	7
1.1     Оптический канал утечки информации .....	8
1.2     Радиоэлектронный канал утечки информации .....	9
1.3     Акустический канал утечки информации .....	10
1.4     Материально-вещественный канал утечки информации .....	10
2     Анализ защищаемых помещений .....	11
2.1     Структура организации .....	11
2.1.1     Обоснование секретности .....	12
2.2     Инженерно-технические показатели объекта .....	13
2.3     Анализ возможных каналов утечки информации .....	16
3     Обоснование защиты информации .....	17
3.1     Руководящие документы .....	17
3.1.1     Федеральные законы РФ .....	17
3.1.2     Указы Президента РФ .....	17
3.1.3     Постановления Правительства РФ .....	18
3.1.4     Специальные нормативно-технические документы ФСТЭК России .....	18
3.2     Требования к защите информации .....	19
4     Анализ технических средств защиты информации .....	22
4.1     Выбор средств защиты .....	24
4.2     Анализ рынка .....	24
4.2.1     Средства пассивной защиты .....	24
4.2.2     Средства активной защиты .....	25
5     Разработка инженерно-технической системы защиты информации .....	28
5.1     Размещение технических средств защиты .....	28
Заключение .....	31
Список литературы .....	32

## **ВВЕДЕНИЕ**

В современном информационном обществе безопасность данных является приоритетной задачей для предприятий. Необходимость защиты от несанкционированного доступа и утечек информации становится все более актуальной, учитывая разнообразные угрозы со стороны конкурирующих предприятий, мошенников, шпионов и других нежелательных пользователей. Утрата или искажение ценной информации может нанести ущерб как репутации, так и финансам компании, подчеркивая важность эффективных методов и средств ее защиты.

Цель данной работы заключается в разработке комплекса инженерно-технической системы защиты информации для организации ООО "Динамика". Объектом защиты является информация, отнесенная к государственной тайне уровня "секретно".

Первая часть работы включает в себя анализ технических каналов утечки информации, вторая часть посвящена анализу организации, помещения и возможным каналам утечки информации, третья – анализу руководящих документов, определяющих рекомендации и требования по защите информации. Последние две части фокусируются на анализе технических средств и их размещении в защищаемых помещениях.

Данная работа необходима, чтобы предоставить комплексное решение для обеспечения конфиденциальности информации и защиты от разнообразных технических каналов утечки данных.

## 1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации есть несанкционированный процесс переноса информации от источника к злоумышленнику.

Техническим каналом утечки информации (ТКУИ) называется совокупность источника конфиденциальной информации, среды распространения информационного сигнала и средств технической разведки (рисунок 1).



Рисунок 1 – Структура технического канала утечки информации

В качестве источников сигналов могут быть:

- объект наблюдения, отражающий электромагнитные волны, в том числе свет;
- объект наблюдения, излучающий собственные электромагнитные волны в оптическом и радиодиапазонах, вызванные тепловым движением электронов;
- движущиеся механизмы и машины, создающие акустические сигналы;
- передатчики функциональных каналов связи;
- ретрансляторы, например закладные устройства;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- радиоактивные материалы.

В контексте изучения ТКУИ выделяют следующие понятия:

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

ОТСС — это непосредственно средства и системы, в которых обрабатывается защищаемая информация.

При выявлении технических каналов утечки информации ОТСС необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами или в защищаемых помещениях.

К ВТСС можно отнести системы пожарной и охранной сигнализации, кондиционирования, оргтехнику, электронные часы и т.п. Если в защищаемом помещении есть телефонная линия, по которой не передается защищаемая информация, она также относится к ВТСС.

"Микрофонный эффект" - нежелательное преобразование акустического сигнала в электрические различные элементы ОТСС и ВТСС. К таким элементам относятся, например, звонковая цепь в телефоне. За счет "микрофонного эффекта" в элементах возникает информационные сигналы, которые злоумышленник может получить с использованием специальных технических средств.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКUI делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

### **1.1 Оптический канал утечки информации**

В оптическом канале информацию передают электромагнитные волны, или фотоны. Одним из способов получения такой информации может быть визуальное наблюдение, например, через окно или приоткрытую дверь. Другой вариант - использование скрытых устройств для фото или видеозаписи. Этот канал представляет интерес, если информация представлена в графической форме.

Для защиты от утечки используются различные методы, такие как установка жалюзи или непрозрачных покрытий на поверхности, видимые снаружи (например, окна, стеклянные двери), а также применение доводчиков для дверей.

Здесь также выделяют оптико-электронный канал утечки информации.



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.

## **1.2 Радиоэлектронный канал утечки информации**

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам из меди, железа, алюминия.

Источниками информационных сигналов в радиоэлектронном канале утечки информации могут быть:

- устройства передачи радиочастотных сигналов, установленные в функциональных каналах связи;
- побочные электромагнитные излучения и наводки (ПЭМИН);
- аппараты, испускающие тепловые электромагнитные волны;
- объекты, способные отражать радиосигналы.

Выделяют следующие радиоэлектронные каналы утечки информации:

- электрические: возникают за счет наводок электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- электромагнитные: возникают за счет физических процессов, происходящих в технических средствах при их функционировании и создающих в окружающем пространстве побочные электромагнитные излучения, которые в той или иной степени связаны с обрабатываемой информацией;
- индукционные: используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации.

Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН).

Защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий электромагнитное излучение технических устройств.

### **1.3 Акустический канал утечки информации**

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.

Выделяют следующие акустические каналы утечки информации:

- виброакустические: средой распространения речевых сигналов являются ограждающие строительные конструкции помещений и инженерные коммуникации. Для перехвата речевых сигналов в этом случае используют вибродатчики (акселерометры);
- электроакустические: утечка информации происходит из-за преобразования звукового сигнала в электрический при прохождении акустических волн через ВТСС;
- параметрические: поле, создаваемое источником акустического сигнала (объектом информации), может изменять параметры электромагнитных устройств, используемых злоумышленниками. Такими устройствами могут быть высокочастотные генераторы с направленными антеннами, радиоприемные установки;
- оптико-акустические: «микрофонный эффект».

### **1.4 Материально-вещественный канал утечки информации**

В материально-вещественном канале утечка информации возможна через несанкционированное распространение за пределы организации вещественных носителей с секретной или конфиденциальной информацией, прежде всего выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат химические элементы, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

## **2 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ**

В рамках анализа защищаемых помещений необходимо рассмотреть область деятельности организации, располагаемой в данном помещении, циркулирующую в ней информацию, а также само помещение, то есть его инженерно-технические показатели.

### **2.1 Структура организации**

Наименование организации: ООО “Динамика”.

Область деятельности: разработка ПО и аналитика систем.

Организационная структура предприятия состоит из следующих подразделений:

- руководство предприятия (директор);
- специалист по ИБ;
- отдел бухгалтерии;
- отдел анализа данных;
- отдел разработки ПО;
- отдел продаж;
- отдел кадров.

Основные информационные процессы:

- предоставление информации об услугах;
- Сбор заявок на аналитику и необходимого информационного сопровождения;
- Предоставление пользователям инструментов для заказа услуги и создания учётной записи на сайте;
- доступ к результатам разработки/аналитики клиенту;
- ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией;
- хранение, обработка, передача, утилизация персональных данных пользователей;
- хранение данных об объемах продаж клиентов;
- хранение данных о внутренних разработках;
- формирование необходимой отчетной и иной статистической документации;
- усовершенствование способов аналитики.

Защищаемая информация:

- коммерческая тайна – сведения о заключенных договорах и контрактах, данные о партнерах и клиентах компании, информация о ценовой политике и финансовых операциях;

– техническая информация конфиденциального характера – состав и структура баз данных, содержащих информацию клиентов, конфигурации используемого серверного и сетевого оборудования, сведения об архитектуре и настройках корпоративных информационных систем;

– государственная тайна – проекты для государственных учреждений или оборонных организаций, информация о разработке систем защиты от киберугроз, криптографии или технологий, обеспечивающих конфиденциальность данных

Потоки информации, циркулирующие в рамках выбранного объекта защиты приведены на рисунке 2. Информационные потоки разделены на открытые и закрытые.

К открытым потокам информации отнесены сведения об открытых вакансиях, а также информация, передаваемая СМИ, для взаимодействия с общественностью, а также информация о материально техническом снабжении.

В закрытых потоках циркулирует информация о внутренней и внешней деятельности, информация из внутренней информационной системы., а также сведения, составляющие государственную тайну.

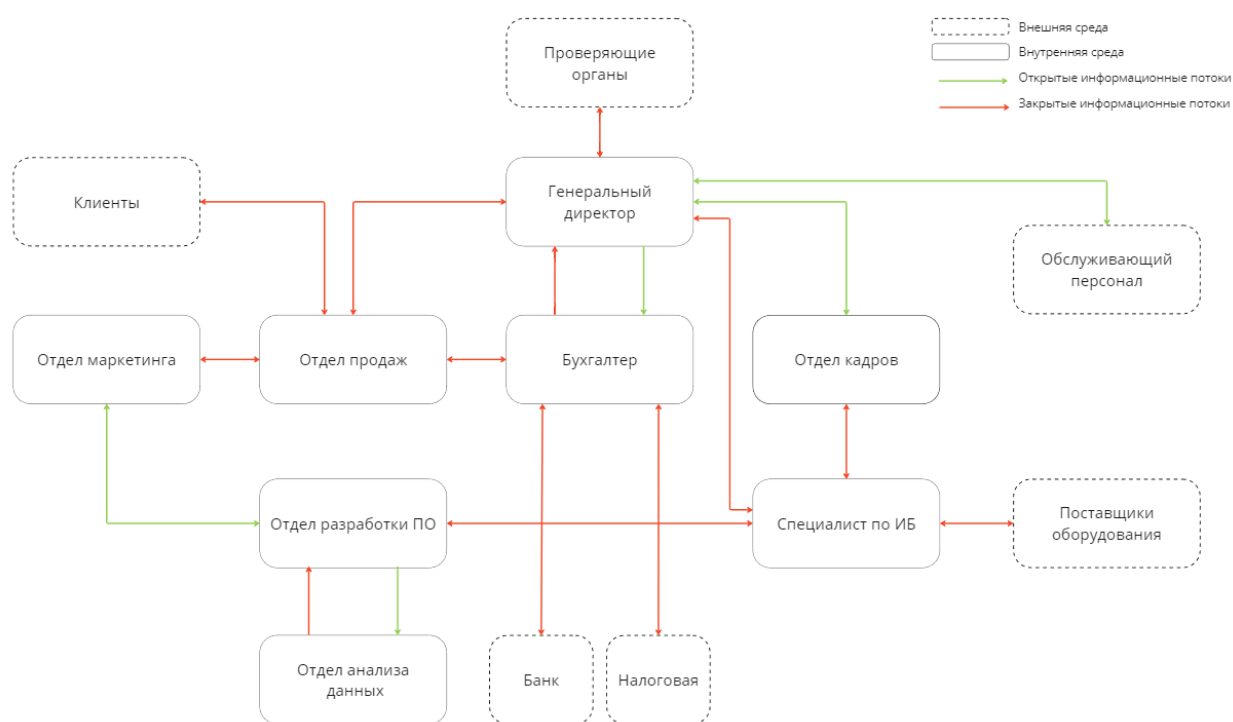


Рисунок 2 – Информационные потоки организации

### 2.1.1 Обоснование секретности

Организация ООО «Динамика» имеет глубокие сведения о системах защиты от киберугроз, а некоторые проекты организации, разрабатываемые для государственных

учреждений, имеют гриф «секретно», поэтому организации необходимо работать со сведениями, составляющими гос. тайну с грифом «секретно», а сотрудникам иметь доступ к этим сведениям.

Как итог, система имеет 3 тип формы доступа для граждан, допускаемых к секретным сведениям.

## 2.2 Инженерно-технические показатели объекта

Рассмотренный в данной курсовом проекте объект защиты представляет собой помещение, расположенное на 6 этаже девятиэтажного здания. План помещения представлен на рисунке 3. Значения условных обозначений указаны в таблице 1.

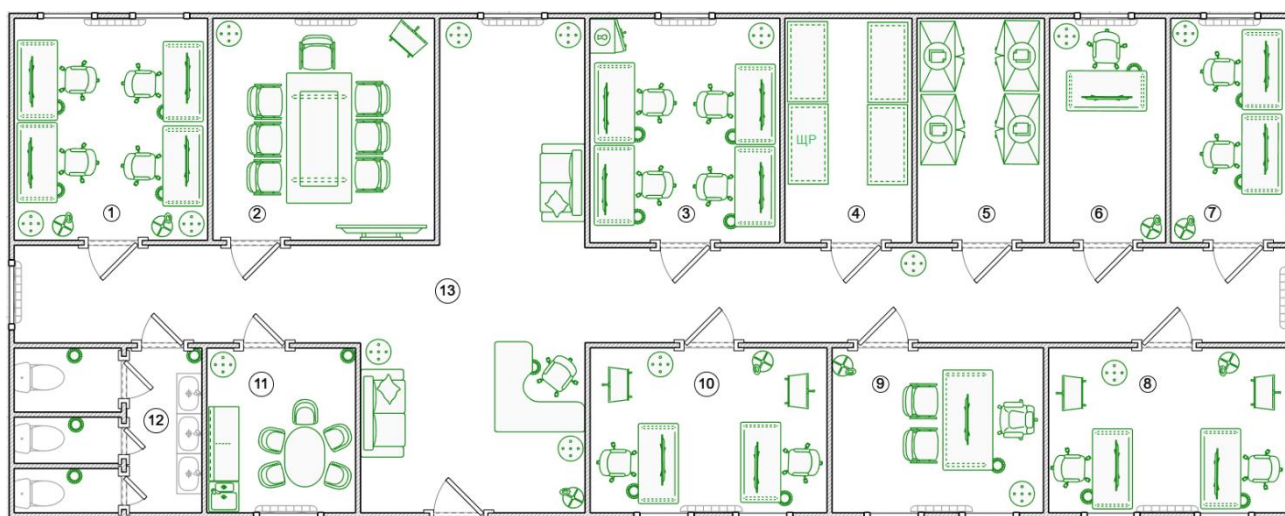


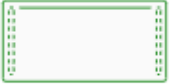













Рисунок 3 – План помещения организации

Помещения на плане пронумерованы в соответствии с названиями:

1. Кабинет отдела разработки (ИТ)
2. Переговорная
3. Кабинет для работы с ГТ
4. Серверная
5. Архив с ГТ
6. Кабинет специалиста по ИБ
7. Кабинет отдела анализа данных
8. Кабинет отдела продаж
9. Кабинет директора
10. Кабинет отдела кадров
11. Кухня
12. Туалет

### 13. Коридор

Таблица 1 – Условные обозначения

Обозначение	Описание
	Рабочий стол
	Стол для переговоров
	Ресепшен-стол
	Стул
	Стул директора
	Стул для переговоров
	Персональный компьютер
	Вешалка
	Горшок с цветами
	Сейф
	Мусорка
	Шкаф с документами
	Сервер
	Щит распределительный

	Раковина
	Батарея
	Телевизор
	Доска
	Диван
	Унитаз
	Кухонная столешница
	Кухонный стул
	Кухонный стол

Помещения, требующие защиты:

1. Переговорная: 4.15м х 4.15м, 17.24м<sup>2</sup>
2. Кабинет директора: 4м х 3.17м, 12.68м<sup>2</sup>
3. IT отдел: 4.15м х 3.74м, 15.52м<sup>2</sup>
4. Кабинет для работы с ГТ: 4.15м х 3.74м, 15.52м<sup>2</sup>
5. Архив с ГТ: 4.15м х 2.43м, 10.08м<sup>2</sup>
6. Серверная: 4.15м х 2.43м, 10.08м<sup>2</sup>
7. Кабинет специалиста по ИБ: 4.15м х 2.15м, 8.92м<sup>2</sup>

Для ведения переговоров предназначено два помещения (кабинет директора и переговорная).

В переговорной находятся: стол, 7 стульев, 1 экран, 6 розеток, 1 батарея центрального отопления, 1 растение, 1 доска.

В кабинете директора: 2 окна, 1 стол, 3 стула, 1 компьютер, 4 розетки, 1 батарея центрального отопления, растение, вешалка для одежды, 1 урна для мусора.

В помещении IT отдела происходит разработка программных продуктов организации.

В IT отделе 2 окна, 1 батарея центрального отопления, 4 рабочих места с ПЭВМ, 8 розеток, 4 урны для мусора, 2 вешалки для одежды, 2 растения.

В кабинете ГТ: 4 рабочих места с ПЭВМ, 8 розеток, 4 урны для мусора, 1 растение, 1 сейф, 1 батарея центрального отопления, 1 окно.

В архиве ГТ: 4 стеллажа с документами, 1 розетка.

В серверной: 4 серверных стойки, 16 розеток.

В кабинете специалиста по ИБ: 1 окно, 1 рабочее место с ПЭВМ, 1 растение, 1 урна для мусора, 1 вешалка для одежды, 1 батарея центрального отопления, 3 розетки.

### **2.3 Анализ возможных каналов утечки информации**

Офис расположен на 6 этаже девятиэтажного здания. Здание одной стороной выходит в закрытый контролируемый двор, другой – на улицу. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. В помещениях присутствуют украшения в виде растений, которые могут использоваться для скрытия скрытых устройств. В каждой комнате имеются электрические розетки, что предоставляет потенциальные каналы для утечки информации через электрические и электромагнитные средства. Существует также угроза сбора информации с использованием вибрационных, оптических, акустических, виброакустических и акустоэлектрических каналов. Касательно материально-вещественного канала утечки информации, следует отметить, что его регулирует строгая политика компании по отношению к физическим носителям информации, данное направление не рассматривается в рамках данной курсовой работы.



### **3 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

Исходя из данных, полученных в предыдущем разделе, организация должна быть защищена, согласно требованиям, выдвигаемым к помещениям, в которых ведется работа со сведениями, составляющими государственную тайну с грифом «секретно».

Также организации необходимо защищать свою коммерческую тайну и сведения о технической реализации ее АС.

Поэтому необходимо рассмотреть руководящие документы по противодействию технической разведке, а также устанавливающие требования по защите сведений, составляющих гос. тайну.

#### **3.1 Руководящие документы**

##### **3.1.1 Федеральные законы РФ**

- Закон РФ от 21.07.1993 №5485–1 "О государственной тайне" (ред. от 15.11.2010);
- Федеральный закон РФ от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации (ред. от 06.04.2011);
- Федеральный закон РФ от 28.12.2010 №390-ФЗ "О безопасности";
- «О связи» от 16 февраля 1995 г. №15-ФЗ.

##### **3.1.2 Указы Президента РФ**

- Указ Президента Российской Федерации №1203 от 30.11.1995 "Об утверждении Перечня сведений, отнесенных к государственной тайне" (ред. от 08.04.2011);
- Указ Президента Российской Федерации №1085 от 16.08.2004 "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка) (ред. От 17.11.2008);
- Указ Президента Российской Федерации от 6.10.2004 г. №1286 "Вопросы Межведомственной комиссии по защите государственной тайны";
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

### **3.1.3 Постановления Правительства РФ**

- Постановление Совета Министров - Правительства Российской Федерации от 15 сентября 1993 года №912–51 "Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам";
- Постановление Правительства Российской Федерации от 3 ноября 1994 года №1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти";
- Постановление Правительства Российской Федерации от 06.02.2010 №63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне";
- Постановление Правительства Российской Федерации от 04.09.1995г. №870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" (ред. от 22.05.2008);
- Постановление Правительства Российской Федерации от 26.06.1995г. №608 "О сертификации средств защиты информации" (ред. от 21.04.2010);
- Постановление Правительства Российской Федерации от 05.01.2004 года №3–1 "Инструкция по обеспечению режима секретности в Российской Федерации";
- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333.

### **3.1.4 Специальные нормативно-технические документы ФСТЭК России**

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

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

### **3.2 Требования к защите информации**

Рассмотрим основные требования к защите, устанавливаемые вышеперечисленными руководящими документами.

Из статьи 27 ФЗ РФ "О государственной тайне" N 5485-1: допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством

Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

При этом Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается при наличии у них сертифицированных средств защиты информации.

Из статьи 28 ФЗ РФ "О государственной тайне" N 5485-1: средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Из пункта 10 Постановления Правительства РФ от 15.04.1995 N 333: специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Из пункта 26 статьи 3 Постановления Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51: защита информации осуществляется путем:

- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;
- выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными

решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Из пункта 4.2. СТР-К. Специальных требований и рекомендаций по технической защите конфиденциальной информации: защищаемые помещения должны размещаться в пределах КЗ. При этом рекомендуется размещать их на удалении от границ КЗ, обеспечивающем эффективную защиту, ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий).

Не рекомендуется располагать ЗП на первых этажах зданий.

Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности прослушивания ведущихся в нем разговоров из-за пределов ЗП.

Из пункта 5.1. СТР-К. Специальных требований и рекомендаций по технической защите конфиденциальной информации: в качестве основных мер защиты информации рекомендуются:

- использование сертифицированных средств защиты информации;
- развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация.

Из требований «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: 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.

#### **4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Исходя из данных, приведенных в пункте 2, можно выделить следующие актуальные технические каналы утечки информации:

- оптические:
  - прямой;
  - оптико-электронный;
- радиоэлектронные:
  - электрический;
  - электромагнитный;
  - индукционный;
- акустические:
  - прямой;
  - виброакустический;
  - электроакустический.

Опираясь на требования к устанавливаемой защите, сформированные в предыдущем разделе, выберем необходимые средства защиты для реализации этих требований.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна с грифом «секретно», – требуется оснастить помещение активными и пассивными средствами защиты информации.

Цель пассивной защиты – максимально ослабить сигнал от источника информативного сигнала, за счет возведения инженерных конструкций. Примером может быть отделка стен звукопоглощающими материалами, экранирование технических средств, установка двойных окон.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

В таблице 2 представлены активные и пассивные средства защиты.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустические (прямой, электроакустический)	проводка, двери, окна, щели в стенах, вентиляция	усиленная звукоизоляция, в том числе вентиляции, доводчики на двери, утолщение дверей, фильтры для сетей электропитания	устройства акустического зашумления
виброакустический, оптико-электронный	батареи, трубы, стены, пол, окна, двери	изолирующие звук и вибрацию обшивки стен, дополнительные поглощающие накладки на радиаторы и трубы тепло- и водоснабжения	устройства вибрационного зашумления
радиоэлектронные (электромагнитный, электрический, индукционный)	ПЭВМ, бытовые приборы, телевизоры, розетки	фильтр для сетей электропитания, экранирование помещения, осуществление развязки по цепям питания	устройства электромагнитного зашумления
прямой оптический	окна, двери	жалюзи на окна, затемненное остекление, доводчики на двери, правильная планировка (экраны	блокирующие обзор устройства

		ПЭВМ не расположены в прямой видимости)	
--	--	---	--

#### **4.1 Выбор средств защиты**

Основываясь на результатах предыдущего пункта, мною были выбраны следующие средства защиты от утечек по техническим каналам:

1. Защита от оптических каналов:
  - а. пассивная:
    - жалюзи или шторы (для помещений без ГТ);
  - б. активная:
    - система виброакустического зашумления категории не ниже 1В (для помещений с ГТ);
2. Защита от акустических каналов:
  - а. пассивная:
    - усиленные двери;
    - обшивка стен звукоизолирующими материалами;
  - б. активная:
    - система виброакустического зашумления категории не ниже 1В;
3. Защита от радиоэлектронных каналов:
  - а. пассивная:
    - сетевые фильтры
  - б. активная:
    - система электромагнитного зашумления

#### **4.2 Анализ рынка**

После выбора средств защиты необходимо определиться с конкретной моделью устройства. Для этого нужно проанализировать рынок и найти наилучшее предложение.

##### **4.2.1 Средства пассивной защиты**

Жалюзи и шторы одинаково защищают от оптического канала утечки информации, поэтому, как наиболее дешевый и удобный в использовании вариант были выбраны горизонтальные пластиковые жалюзи Эскар стоимостью 630 рублей за единицу 50x160см.



В результате анализа рынка усиленных дверей, в розничной торговле был найден лишь один вариант двери, удовлетворяющий требованиям грифа «секретно»: противопожарная EI 60 стоимостью 31 000 рублей. В ходе анализа не рассматривался вариант создания двери под заказ.

В результате анализа рынка сетевых фильтров была выявлена модель, являющаяся наиболее популярной среди покупателей в разных магазинах: сетевой фильтр Power Cube SPG-B-10. Данная модель отличается надежностью и небольшой ценой в 1000 рублей.

#### 4.2.2 Средства активной защиты

Сравнительный анализ систем виброакустического зашумления представлен в таблице 3.

Таблица 3 – Сравнительный анализ систем виброакустического зашумления

	<b>ЛГШ-404</b>	<b>ЛГШ-403</b>	<b>ЛГШ-402</b>	<b>ANG-2000</b>
Сертификация и соответствие требованиям	Соответствует требованиям 2 класса защиты	Соответствует требованиям по 3-му классу защиты	Соответствует требованиям по 4-му классу защиты	Соответствует требованиям 2 класса защиты
Генератор шума	Есть. Размеры 188 х 160 х 60 мм	Есть. Размеры 82 х 67 х 22 мм.	Есть. Размеры 145 х 100 х 50 мм.	Есть. Размеры 43 х 152 х 254 мм
Вибропреобразователи	Габаритные размеры не более 40 х 25 мм	Габаритные размеры не более 40 х 25 мм	Габаритные размеры не более 40 х 25 мм	Габариты 102 х 38 мм
Акустические излучатели	Габаритные размеры не более 66 х 66 х 25 мм	Габаритные размеры не более 66 х 66 х 25 мм	Габаритные размеры не более 66 х 66 х 25 мм	Габариты 127 х 146 мм
Диапазон рабочих частот	175 / 11200 Гц	170 / 12 900 Гц	175 / 11 200 Гц	250 / 5 000 Гц.
Интервал уровня	Не менее 15 дБ	не менее 40 дБ	Не менее 35 дБ	Не менее 40 дБ

регулировки звукового давления				
Цена	35 100 руб.	19 400 руб.	18 200 руб.	14 350 руб.

По результатам анализа была выбрана ЛГШ-403. Она имеет наименьший класс защиты, среди представленных моделей, однако его достаточно для соответствия требованиям к грифу «секретно». Данная система имеет наибольший диапазон зашумления, а также малые габариты, что, в сумме с остальными ее характеристиками делает ее лучшей системой из представленных.

В состав ЛГШ-403 входят:

- Генератор шума ЛГШ-403 (6000 руб.);
- Вибропреобразователь для стен, полов, потолков ЛВП-2с (3640 руб.);
- Вибропреобразователь для окон ЛВП-2о (3640 руб.);
- Акустический излучатель ЛВП-2а (3640 руб.);
- Вибропреобразователь для трубопроводов ЛВП-2т (3640 руб.);
- Размыкатели ЛУР (5 590 руб.).

Сравнительный анализ систем виброакустического зашумления представлен в таблице 4.

Таблица 4 – Сравнительный анализ систем электромагнитного зашумления

	<b>ЛГШ - 503</b>	<b>ЛГШ-505</b>	<b>ЛГШ-513</b>
Соответствует требованиям документов	Соответствует требованиям по 2-му классу защиты	Соответствует требованиям по 2-му классу защиты	Соответствует требованиям по 2-му классу защиты
Диапазон частот	0,01–1800 МГц	0,01 МГц – 1000 МГц	0,009–1800 МГц
Диапазон регулировки уровня шума	Не менее 20 дБ	Не менее 50 дБ	Не более 20 дБ
Потребляемая мощность	Не более 45 ВА	не более 55 Вт	Не более 45 ВА
Цена	44 200 руб.	27 660 руб.	39 000 руб.

По итогу сравнительного анализа было выбрано устройство ЛГШ-513. Несмотря на то, что модель ЛГШ-505 дешевле, она имеет характеристики, значительно уступающие характеристикам выбранной модели. Тем не менее, конечная цена является приемлемой, так как данное устройство обеспечивает защиту от электрических и электромагнитных каналов утечки, а также предотвращает ПЭМИН.

## **5 РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

В результате анализа, проведенного в предыдущем разделе, были выбраны следующие конкретные средства защиты:

- Система постановки виброакустических и акустических помех ЛГШ-403;
- Генератор шума ЛГШ-513;
- Жалюзи;
- Сетевые фильтры;
- Усиленные двери.

ЛГШ-513 имеет визуальную систему индикации нормального режима работы и визуально-звуковую систему индикации аварийного режима (отказа).

Рекомендации по установке ЛГШ-403:

- для стен: один вибропреобразователь ЛВП-2с на каждые 6 м<sup>2</sup>;
- для полов и потолков: один вибропреобразователь ЛВП-2с на каждые 6 м<sup>2</sup>;
- для окон: один вибропреобразователь ЛВП-2о на каждое стекло;
- для трубопроводов: один вибропреобразователь ЛВП-2т на каждый независимый участок инженерно-технических коммуникаций (например, водопровод и т.д.);
- для воздуховодов, вентиляции, двойных дверных коробок и прочих замкнутых объемов: по одному акустическому излучателю ЛВП-2а на каждые 40 м<sup>3</sup> каждого замкнутого объема.

### **5.1 Размещение технических средств защиты**

На основе результатов, полученных на всех предыдущих этапах работы, была разработана инженерно-техническая система защиты информации для организации ООО «Динамика». Состав и размещение инженерно-технических средств защиты информации представлен на рисунке 3. Описание условных обозначений средств защиты представлено в таблице 5. В таблице 5 также указаны цены и количество СЗИ, а также итоговая стоимость установленных средств защиты.

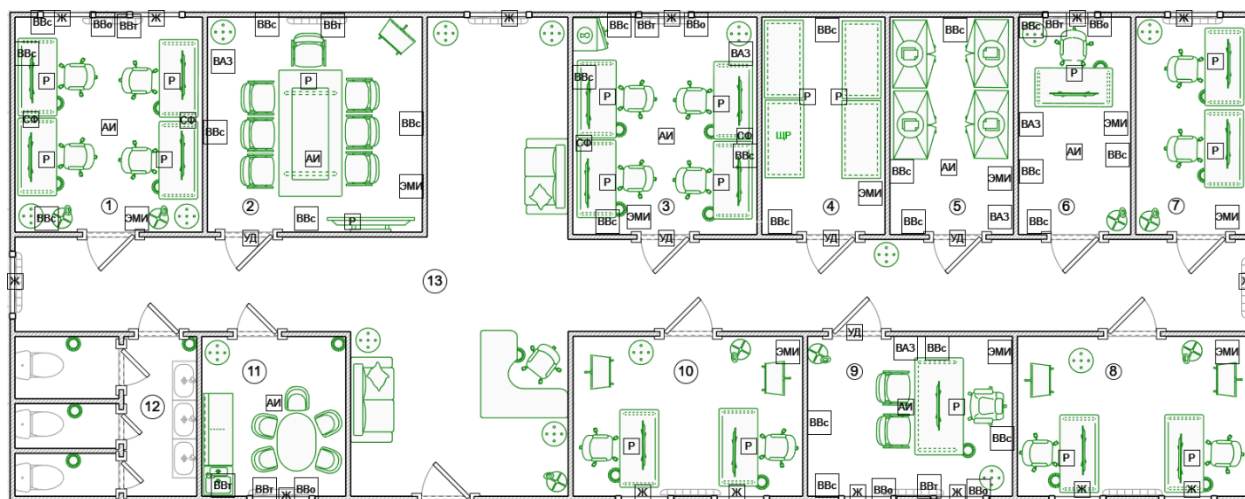


Рисунок 4 – План помещения предприятия с инженерно-технической системой защиты информации

Таблица 5 – Условные обозначения средств защиты

Обозначение средства защиты	Описание	Цена, руб.	Количество	Общая стоимость, руб.
ВВс	Вибропреобразователь для стен, полов, потолков ЛВП-2с	3 640	24	87 360
ВВо	Вибропреобразователь для окон ЛВП-2о	3 640	6	21 840
АИ	Акустический излучатель ЛВП-2а	3 640	7	25 480
ВВт	Вибропреобразователь для трубопроводов ЛВП-2т	3 640	7	25 480
Р	Размыкатели ЛУР	5 590	20	111 800
ВАЗ	Генератор зашумления ЛГШ-403 (виброакустическое зашумление)	6 000	5	30 000
ЭМИ	Генератор зашумления ЛГШ-513 (электромагнитное излучение)	39 000	10	390 000
СФ	Сетевой помехоподавляющий фильтр	1 000	4	4 000
Ж	Жалюзи	630	15	9 450

УД	Усиленная дверь	31 000	5	155 000
<b>Итого</b>				<b>860 410</b>

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был проведен анализ существующих технических каналов утечки информации для защищаемого помещения организации ООО "Динамика", занимающейся работой с государственной тайной уровня "секретно". Выявленные каналы включали акустический, оптический, акустоэлектрический, электрический, электромагнитный, оптико-электронный технические каналы, а также потенциальные угрозы ПЭМИН.

На основе проведенного анализа была разработана инженерно-техническая система защиты информации для данной организации. Предпроектное обследование включало анализ информационных активов, как внутренних, так и внешних, а также оценку открытых и закрытых информационных потоков. Помещение организации было тщательно обследовано для выявления возможных каналов утечки информации.

Дополнительно был проведен анализ нормативной базы, подтверждающей необходимость защиты информации, и изучен рынок инженерно-технических средств, чтобы выбрать оптимальные решения. На основе этих данных был разработан план установки выбранных средств, а также подсчитаны затраты на их приобретение.

В итоге была успешно достигнута цель работы – разработка и внедрение инженерно-технической системы защиты информации для ООО "Динамика". Все поставленные задачи были выполнены, и организация теперь обеспечена надежной защитой от потенциальных угроз утечки информации через различные технические каналы.

## СПИСОК 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: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 14.09.2023)
5. Требования к режимным помещениям и их оборудованию // Компания КАСЛ-ЦЛС Прогресс URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam> (дата обращения: 25.11.2023)