

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

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Инженерно-технические средства защиты информации»

**КУРСОВОЙ ПРОЕКТ**

на тему:

«Проектирование инженерно-технической системы защиты информации на  
предприятии. Вариант 149»

**Выполнила:**

Кочнева Екатерина Михайловна,  
бакалавр группы N34532



---

(подпись)

**Проверил:**

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

---

(подпись)

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

**Студент** Кочнева Екатерина Михайловна

(Фамилия И.О.)

**Факультет** Безопасности Информационных Технологий

**Группа** N34532

**Направление (специальность)** 11.03.03 – Технологии защиты информации (2020)

**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

**Задание** Проанализировать всевозможные каналы утечки данных в помещении, провести  
анализ рынка технических средств защиты информации разных категорий, разработать схему  
расстановки выбранных технических средств в защищаемом помещении

**Краткие методические указания**

**Содержание пояснительной записки** Курсовая работа содержит введение, организационную  
структуру предприятия, обоснование защиты информации, описание помещения, анализ рынка  
технических средств, рекомендации по организации защиты, заключение, список источников

**Рекомендуемая литература** Кармановский Н.С., Михайличенко О.В., Савков С.В.

Организационно-правовое и методическое обеспечение информационной безопасности

Учебное пособие / СПб: НИУ ИТМО, 2013-148с.

**Руководитель** Попов Илья Юрьевич

(Подпись, дата)

**Студент** Кочнева Екатерина Михайловна

06.11.2023

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент** Кочнева Екатерина Михайловна

(Фамилия И.О.)

**Факультет** Безопасности Информационных технологий

**Группа** N34532

**Направление (специальность)** 11.03.03 – Технологии защиты информации (2020)

**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

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и согласование ТЗ	24.10.2023	24.10.2023	
2	Анализ источников информации	26.10.2023	26.10.2023	
3	Работа над курсовой работой	04.11.2023	04.11.2023	
4	Оформление отчета по курсовой работе	06.11.2023	06.11.2023	
5	Защиты курсовой работы	09.11.2023	19.12.2023	

**Руководитель** Попов Илья Юрьевич

(Подпись, дата)

**Студент** Кочнева Екатерина Михайловна 06.11.2023

(Подпись, дата)

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Кочнева Екатерина Михайловна
	(Фамилия И.О.)
<b>Факультет</b>	Безопасности Информационных технологий
<b>Группа</b>	N34532
<b>Направление (специальность)</b>	11.03.03 – Технологии защиты информации (2020)
<b>Руководитель</b>	Попов Илья Юрьевич, к.т.н., доцент ФБИТ университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Проектирование инженерно-технической системы защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА  
(РАБОТЫ)**

**1. Цель и задачи работы**

- Предложены студентом
- Сформулированы при участии студента
- Определены руководителем

**Цель:** разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

**Задачи:** рассмотреть организационную структуру предприятия; обосновать необходимость защиты информации; провести анализ защищаемых помещений; выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений; спроектировать систему защиты информации на основе выбранных средств.

## 2. Характер работы

- Расчет
- Конструирование
- Моделирование
- Другое

## 3. Содержание работы

Курсовая работа содержит введение, организационную структуру предприятия, обоснование защиты информации, анализ защищаемых помещений, анализ рынка предлагаемых решений, описание расстановки технических мер защиты информации, заключение, список источников.

## 4. Выводы

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

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Кочнева Екатерина Михайловна 06.11.2023

(Подпись, дата)

«\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

## СОДЕРЖАНИЕ

Введение.....	3
1     Организационная структура предприятия.....	5
2     Обоснование защиты информации .....	8
3     Анализ защищаемых помещений.....	11
3.1   План помещений предприятия.....	11
3.2   Описание помещений.....	15
3.3   Анализ потенциальных каналов утечек информации .....	17
3.4   Выбор средств защиты информации.....	17
4     Анализ рынка предлагаемых решений .....	19
4.1   Устройства для перекрытия акустического и виброакустического каналов утечки информации .....	19
4.2   Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации .....	23
4.3   Устройства для перекрытия визуально-оптического канала утечки информации.....	27
5     Описание расстановки технических мер защиты информации .....	28
Заключение .....	32
Список использованных источников .....	33

## **ВВЕДЕНИЕ**

В настоящее время, в условиях стремительного развития информационных технологий и все большей зависимости организаций от электронной обработки, хранения и передачи данных, обеспечение безопасности информации становится одной из наиболее актуальных и важных задач. Особенно это касается предприятий, которые работают с конфиденциальной и важной информацией, включая персональные данные клиентов, финансовые отчеты, коммерческие секреты и другие конфиденциальные данные. В этом контексте проектирование инженерно-технической системы защиты информации на предприятии играет фундаментальную роль в обеспечении безопасности данных и предотвращении различных угроз.

В работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации на объекте: государственная тайна с уровнем «секретно». Объект имеет 8 помещений, в которые входят серверное помещение, кабинет руководителей, кабинет генерального директора, кабинет для совещаний и переговоров, кабинет бухгалтерии, открытое рабочее пространство, кухонная зона и санузел.

Цель работы – разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- Рассмотреть организационную структуру предприятия;
- Обосновать необходимость защиты информации;
- Провести анализ защищаемых помещений;

- Выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений;
- Спроектировать систему защиты информации на основе выбранных средств.



# 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Предприятие – объект, обрабатывающий материальные или информационные потоки. Организационная структура предприятия – это формальная система, которая определяет, как управляются и координируются различные функциональные направления, подразделения и индивиды в организации. Схема организационной структуры защищаемого предприятия представлена на рисунке 1.

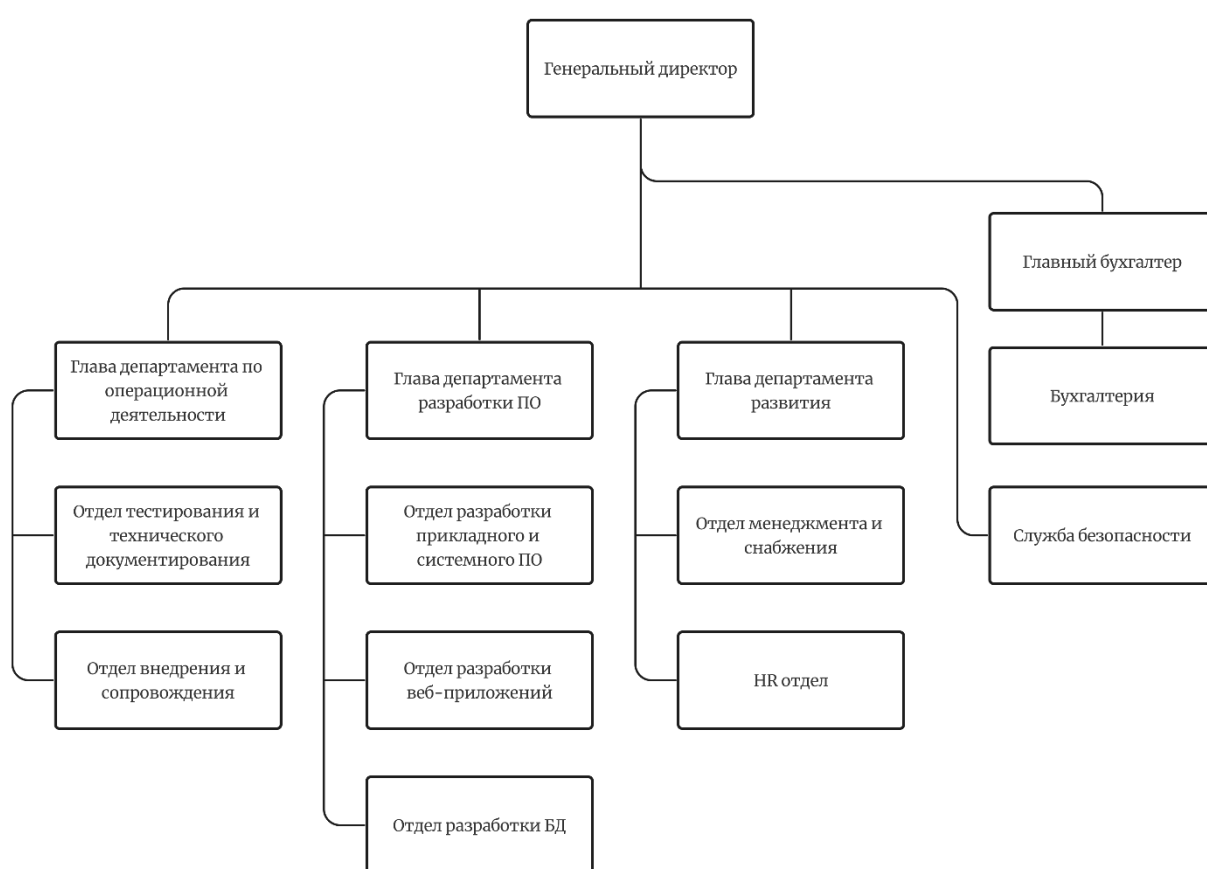


Рисунок 1 – Организационная структура предприятия

Информационные потоки представляют собой ключевую составляющую системы передачи данных в организации или процессе. Схема информационных потоков позволяет визуализировать и описать обмен информацией между различными участниками системы. Она помогает выявить и проанализировать все этапы передачи и обработки информации,

идентифицировать узкие места и возможные проблемы в потоке данных, а также оптимизировать процессы коммуникации и обработки информации. Схема информационных потоков предприятия представлена на рисунке 2.

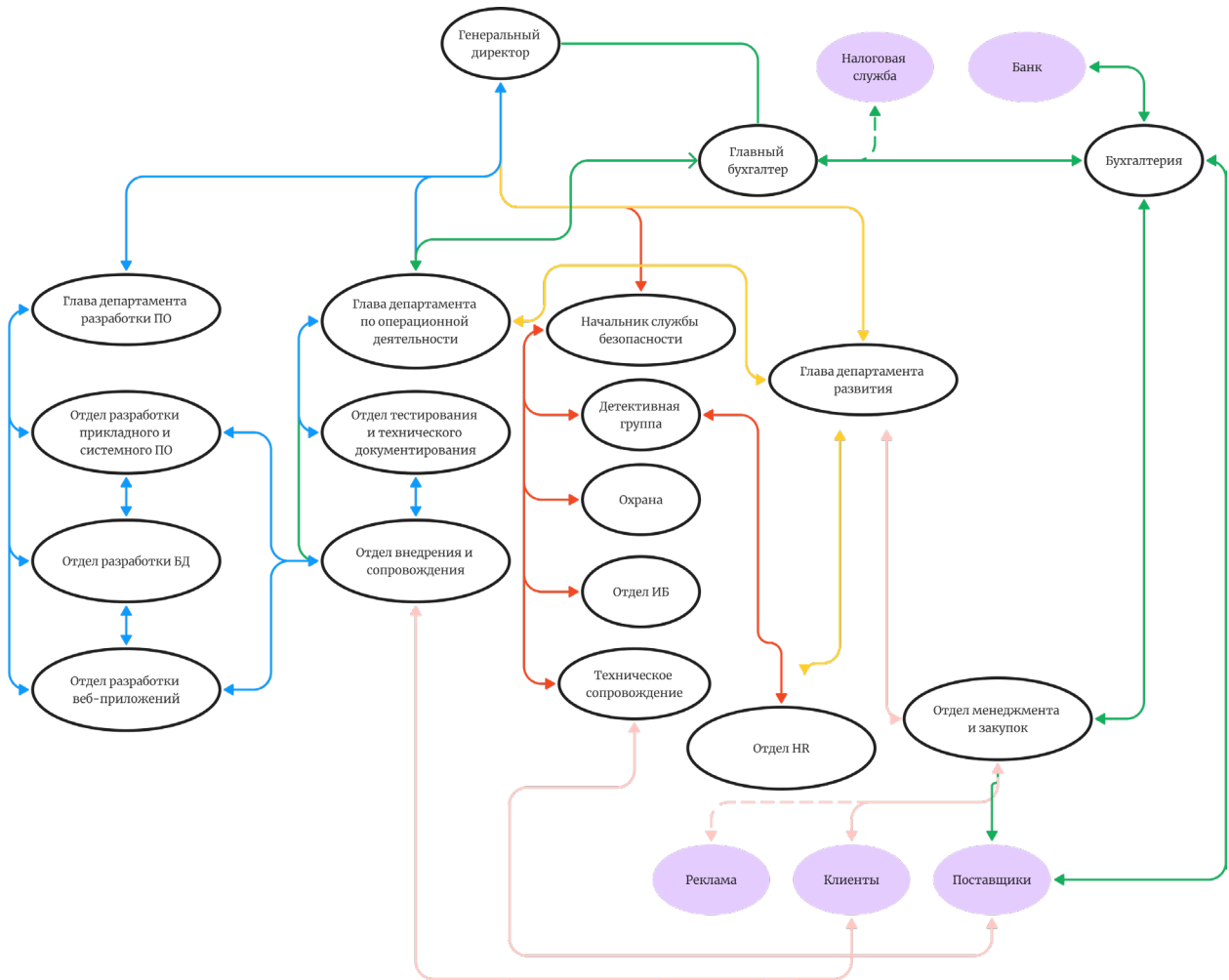



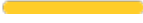

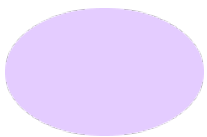



Рисунок 2 – Информационные потоки предприятия

Пояснения к цветовым обозначения на схеме информационных потоков предприятия представлены в таблице 1.

Таблица 1 – Цветовые обозначения на рисунке 2

Обозначение	Значение
	Информация, связанная с основной деятельностью предприятия – разработкой информационных продуктов
	Информация, связанная с финансовой деятельностью предприятия

	Информация, связанная с обеспечением информационной и физической безопасности предприятия
	Информация, связанная с обеспечением оптимального функционирования основной деятельности предприятия
	Информация, связанная с внешним взаимодействием предприятия на рынке
	Внешние субъекты информационного обмена предприятия
	Внутренние субъекты информационного обмена предприятия

Пунктирной линией на схеме обозначены открытые информационные потоки – к ним относятся связи между главным бухгалтером и налоговой службой, а также между отделом менеджмента и закупок и рекламой.

Остальные информационные потоки являются закрытыми, поскольку содержат в себе один (или несколько) видов защищаемых активов:

- Персональные данные сотрудников и клиентов;
- Секретные сведения, содержащие государственную тайну;
- Конфиденциальная информация, содержащая коммерческую тайну.

## **2      ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

Государственная безопасность – система гарантий государства от угроз извне и основам конституционного строя внутри страны. Для реализации этих гарантий в стране создана и функционирует система защищаемых законом тайн. Под тайной понимается нечто скрываемое от других, известное не всем, секрет. Существует большое число охраняемых законом тайн.

В информации, хранящейся и обрабатываемой защищаемым объектом, содержатся сведения, содержащие:

1. Коммерческую тайну – информацию, которая относится к бизнес-операциям, процессам, методологиям и стратегиям предприятия, и которая дает ей конкурентное преимущество на рынке. Это могут быть конфиденциальные данные о продуктах, клиентах, партнерах, сделках, финансовых показателях, исследованиях и разработках.
2. Персональные данные – предприятие обрабатывает персональные данные сотрудников, клиентов и сторонних лиц, работающих с проектами. Это может включать личную информацию, такую как имена, адреса, номера телефонов, электронные адреса, финансовые данные, данные о физической и медицинской характеристиках и другие личные сведения.
3. Государственную тайну – это сведения политического, экономического, военного и научно-технического характера, утрата или разглашение которых создает угрозу безопасности и независимости государства или наносит ущерб его интересам.

Подробнее остановимся на государственной тайне. Установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической,

разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

В рассматриваемом предприятии фигурируют сведения второй степени секретности (гриф «секретно»). Предприятие занимается разработкой программного обеспечения, обеспечивающего шифрование данных.

На основании представленной выше информации, требования к защите информации определяют следующие руководящие документы:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
5. Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
6. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
7. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
8. Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;
9. Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними";
10. СТР. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
11. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.

### 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

#### 3.1 План помещений предприятия

Перед началом проектирования инженерно-технической защиты подробно рассмотрим план помещений с меблировкой предприятия (рисунок 3).






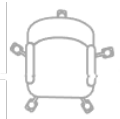





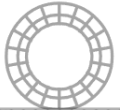


Рисунок 3 – План защищаемого помещения

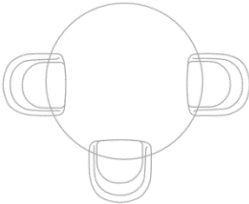

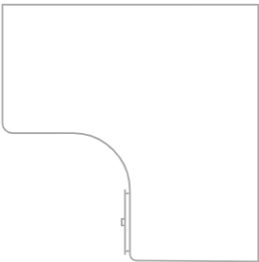
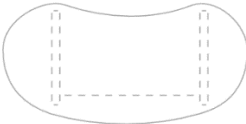





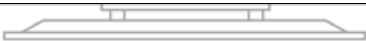
Описание условных обозначений на плане представлено в таблице 2.

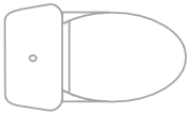
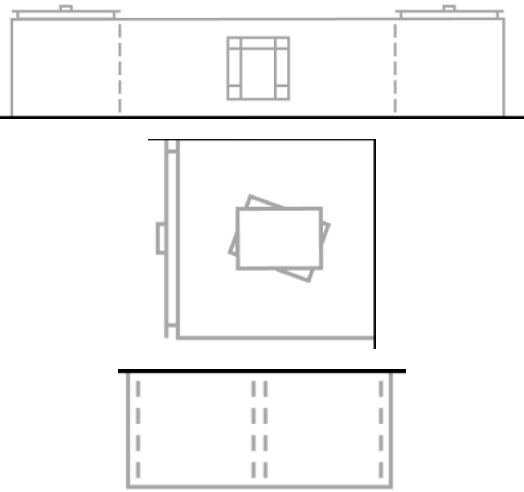

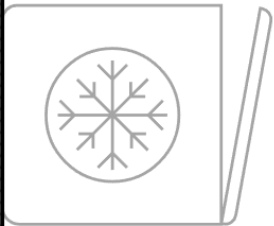

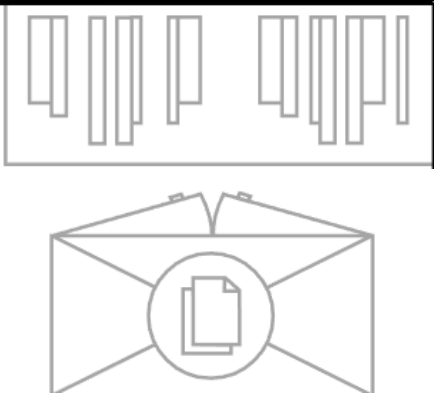
Таблица 2 – Условные обозначения на плане защищаемого помещения

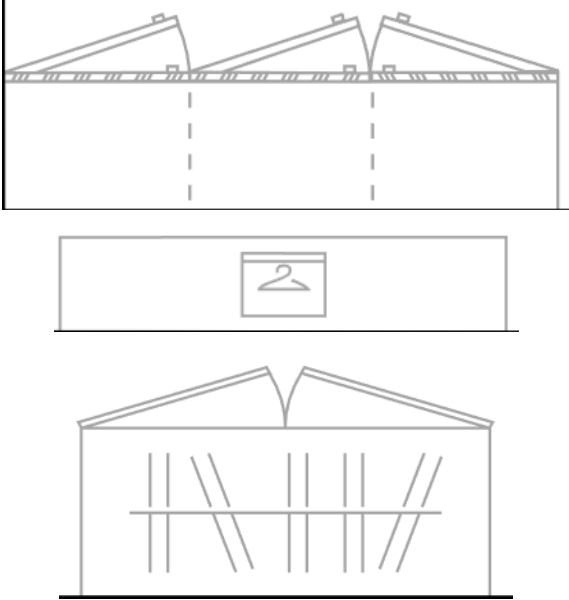
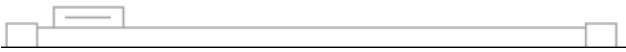



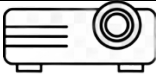
Графическое изображение		Наименование
		Вешалка напольная
		Дверной проем
		Диван

	
	Журнальный столик
	Кофемашина
     	Кресло и стул
	Куллер для воды
	Микроволновая печь
	Корзина для мусора



	Обеденный стол со стульями
	Оконный проем
  	Рабочий стол
	Радиатор отопления
	Раковина
	Санитайзер
	Стол для переговоров и совещаний
	Телевизор

	Туалет
	Тумбочка
	Флипчарт
	Холодильник
	Чайник
	Шкаф

	
	Экран для проектора
	Розетка
	Серверный шкаф
	Цветочный горшок
	Проектор

### 3.2 Описание помещений

На плане обозначены 8 комнат, из них подлежат защите помещения под номерами 1–7:

1. Серверное помещение, 5.5м x 3.22м (17.7м<sup>2</sup>)
2. Кабинет управляющих, 4.9м x 4.2м (20.6м<sup>2</sup>)
3. Кабинет генерального директора, 4.9м x 4.2м (20.6м<sup>2</sup>)
4. Комната для переговоров и совещаний, 4.9м x 6.9м (33.8м<sup>2</sup>)

5. Кабинет бухгалтерии, 4.9м x 4.2м (20.6м<sup>2</sup>)
6. Открытое рабочее пространство, 136м<sup>2</sup>
7. Кухонная зона, 4м x 8.9м (35.6 м<sup>2</sup>)

В серверном помещении расположены: рабочий стол, стул, персональный компьютер, электрический щиток, три серверных шкафа и три розетки. Окон в помещении нет.

В кабинете управляющих расположены: три рабочих стола, три стула, три персональных компьютера, два шкафа, три розетки, комнатное растение, куллер для воды, напольная вешалка, корзина для мусора. В помещении одно окно и один радиатор отопления.

В кабинете генерального директора расположены: рабочий стол, три стула, персональный компьютер, две тумбочки, диван, куллер для воды, телевизор и две розетки. В помещении одно окно и один радиатор отопления.

В комнате для переговоров и совещаний расположены: стол, десять стульев, шкаф, тумбочка, куллер для воды, проектор, экран для проектора, флипчарт, две розетки. В помещении два окна и два радиатора отопления.

В кабинете бухгалтерии расположены: рабочий стол, пять стульев, четыре персональных компьютера, три шкафа, тумбочка, две розетки, комнатное растение, куллер для воды, напольная вешалка, корзина для мусора. В помещении одно окно и один радиатор отопления.

В открытом рабочем пространстве расположены: семь рабочих столов, двадцать пять стульев, семнадцать персональных компьютеров, три шкафа, диван, два кресла, журнальный стол, два куллера для воды, двенадцать розеток, два комнатных растения, санитайзер. В помещении три окна и два радиатора отопления.

В кухонной зоне расположены: четыре обеденных стола, десять стульев, раковина, холодильник, микроволновая печь, электрический чайник,

кофеварка, корзина для мусора, две розетки. В помещении одно окно и два радиатора отопления.

Офис расположен на третьем этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

### **3.3 Анализ потенциальных каналов утечек информации**

В помещениях рассматриваемого объекта присутствуют декоративные элементы, в которых можно спрятать закладное устройство. В каждом помещении имеются розетки и сетевые устройства, а в некоторых и телеаппаратура, значит актуальны утечки через электрический и электромагнитный каналы. Также есть угроза снятия информации через вибрационный (включая виброакустический), оптический и акустический (включая акустоэлектрический) каналы. Материально-вещественный канал в рамках данной работы не рассматривается, поскольку его защита регламентируется внутренней политикой информационной безопасности компании.

### **3.4 Выбор средств защиты информации**

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещения средствами инженерно-технической защиты (таблица 3).

Таблица 3 – Средства защиты для различных каналов утечки

Канал утечки	Источники	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка, вентиляция	Звукоизоляция помещений, акустические экраны, фильтры для цепей электропитания	Акустические извещатели
Вибрационный, виброакустический	Радиаторы отопления, любые твердые поверхности в помещениях	Изоляция поверхностей за счет дополнительной обшивки, наличие тамбура	Вибрационные извещатели
Оптический	Окна, двери	Средства преграждения отраженного света, доводчики на дверях	Маскирующие средства сокрытия объектов
Электромагнитный, электрический	Розетки, АРМ, любые электрические приборы	Фильтры для цепей электропитания, экранирование металлическим материалом	Системы линейного и пространственного зашумления

## **4 АНАЛИЗ РЫНКА ПРЕДЛАГАЕМЫХ РЕШЕНИЙ**

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

- 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.
- Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
- Все режимные помещения оборудуются аварийным освещением.
- 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.

### **4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации**

Для пассивной защиты объекта используются следующие средства:

- Усиленные двери;

- Тамбурное помещение перед переговорной;
- Дополнительная отделка переговорной звукоизолирующими материалами.

В качестве средств для активной защиты используется система виброакустического зашумления. Для защиты помещения, предназначенного для работы с государственной тайной уровня «секретно», будут рассмотрены средства активной защиты информации для объектов информатизации не ниже 1Б. В таблице 4 приведен сравнительный анализ решений, предлагаемых на современном рынке, и удовлетворяющих указанным требованиям для защиты объекта от утечек по виброакустическому каналу.

Таблица 4 – Средства активной защиты от утечек по виброакустическому каналу

Фирма	Устройство	Цена, руб.	Характеристики
ППШ	Система постановки виброакустических и акустических помех «ЛГШ-404»	35 100	<ul style="list-style-type: none"> <li>• Диапазон рабочих частот 175...11200 Гц</li> <li>• Потребляемая мощность 25 Вт</li> <li>• Электропитание 220 В, 50 Гц</li> <li>• Габаритные размеры генераторного блока 188x160x60 мм</li> <li>• Количество подключаемых</li> </ul>



			излучателей на канал до 20 шт.
ППШ	Виброзэкран «ЛИСТ-1»	16 380 – 45 240	<ul style="list-style-type: none"> <li>Размеры 200–2900 мм</li> </ul>
НПО Анна	Аппаратура защиты от акустической разведки «Соната АВ» модель 4Б	44 200	<ul style="list-style-type: none"> <li>Диапазон рабочих частот 90...11200 Гц</li> <li>Потребляемая мощность до 40 Вт</li> <li>Электропитание 220 В, 50 Гц</li> <li>Габариты блока, не более 142х60х167 мм</li> <li>Количество подключаемых излучателей на канал до 239 шт.</li> </ul>
НПП «Гамма»	Система виброакустической защиты "Гамма СВАЗ-01"	64 920	<ul style="list-style-type: none"> <li>Диапазон рабочих частот соответствует защите выделенных помещений до 1 категории включительно</li> <li>Потребляемая мощность до 80 Вт</li> </ul>

			<ul style="list-style-type: none"> <li>• Электропитание 220 В, 50 Гц</li> <li>• Количество подключаемых излучателей на канал до 60 шт.</li> </ul>
НПП «Гамма»	Система постановки виброакустических и акустических помех «ШОРОХ-5Л»	21 500	<ul style="list-style-type: none"> <li>• Диапазон рабочих частот 20...20000 Гц</li> <li>• Потребляемая мощность до 80 Вт</li> <li>• Электропитание 220 В, 50 Гц (есть возможность работы системы от источника питания 12 В)</li> <li>• Количество подключаемых излучателей на канал до 35 шт.</li> </ul>

В результате сравнения, в качестве применяемого решения была выбрана аппаратура защиты от акустической разведки «Соната АВ» модель 4Б. Данный выбор обоснован оптимальным соотношением цены и выдаваемых характеристик системы. Система предоставляет возможность построения системы автоматического контроля всех элементов при минимально возможной стоимости оборудования и монтажа, а также возможность изменения настроек генераторов-излучателей "на лету" и, как следствие – возможность построения адаптивной ("многопрофильной")

системы виброакустической защиты, обеспечивающей выполнение требований по защищенности при различных вариантах использования помещения.

#### **4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации**

Для пассивной защиты объекта используются сетевые фильтры для цепей электропитания, экранирование металлическим материалом.

В качестве средств для активной защиты используется генератор пространственного зашумления для создания в сети белого шума, который скрывает колебания, порождаемые работающей электрической техникой или воздействием звуковой волны. В таблице 5 приведен сравнительный анализ решений, предлагаемых на современном рынке, и удовлетворяющих требованиям класса защиты для предотвращения утечек по электрическим каналам.

Таблица 5 – Средства активной защиты от утечек по электрическим каналам

Фирма	Устройство	Цена, руб.	Характеристики
ППШ	Генератор Шума ЛГШ-501	29 900	<ul style="list-style-type: none"> <li>• Энтропийный коэффициент качества шума на выходе генератора не менее 0,8</li> <li>• Спектральная плотность напряженности</li> </ul>

			<p>магнитного поля шума от 10 до 65 дБ</p> <ul style="list-style-type: none"> <li>• Рабочий диапазон частот 0.01 ÷ 1800 МГц</li> <li>• Габаритные размеры, не более 230x110x50 мм</li> <li>• Потребляемая мощность не более 55 Вт</li> </ul>
НПО Анна	Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РЗ.1».	33 120	<ul style="list-style-type: none"> <li>• Спектральная плотность напряженности магнитного поля шума до 60 дБ</li> <li>• Рабочий диапазон частот до 2 ГГц</li> <li>• Габаритные размеры, не более 640x240x240 мм</li> <li>• Потребляемая мощность не более 30 Вт</li> </ul>

ООО «Радиоэлектронные системы»	Генератор шума Покров, исполнение 1	32 800	<ul style="list-style-type: none"> <li>• Рабочий диапазон частот до 6000 МГц</li> <li>• Габаритные размеры, не более 439 х 74 х 53 мм</li> <li>• Потребляемая мощность не более 15 Вт</li> </ul>
	Генератор шума ГНОМ-3М	57 200	<ul style="list-style-type: none"> <li>• Энтропийный коэффициент качества шума на выходе генератора не менее 0,8</li> <li>• Спектральная плотность напряженности магнитного поля шума от 25 до 75 дБ</li> <li>• Рабочий диапазон частот до 1800 МГц</li> <li>• Габаритные размеры, не</li> </ul>

			более 300x192x50 мм • Потребляемая мощность не более 40 Вт
АО «НПО Эшелон»	Генератор шума ПУЛЬСАР	24 525	• Энтропийный коэффициент качества шума на выходе генератора не менее 0,97 • Рабочий диапазон частот до 6 ГГц • Габаритные размеры, не более 150x95x50 мм • Потребляемая мощность не более 50 Вт

В результате сравнения, в качестве применяемого решения было выбрано устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РЗ.1». ПЭМИН «Соната-РЗ.1» обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем

индуцирования в них маскирующих шумовых напряжений. Преимуществом данного решения можно назвать возможность комбинирования нескольких устройств с целью потенциального повышения класса защищенности. Также, что немаловажно, данное устройство имеет сертификат ФСТЭК и приемлемую стоимость. Ещё один фактор, говорящий в пользу данного устройства – выбор средства защиты от акустических утечек от этого же производителя, что дает нам возможность встроить его в систему «Соната АВ-4Б».

#### **4.3 Устройства для перекрытия визуально-оптического канала утечки информации**

Для прекращения функционирования оптического канала утечки информации необходимо установить на окно жалюзи, шторы или тонирующие пленки.

Также решением, которое может обеспечить дополнительную защиту от утечек по виброакустическому каналу, может являться виброэкрэн «Лист-1», рассмотренный в пункте 4.1.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

## **5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ**

На основе информации, приведенной в главе 4, выбранные технические средства защиты информации включают в себя:

- Усиленные двери (от 4 мм), обшитые металлом (от 2 мм) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт., в кабинет управляющих, кабинет генерального директора, переговорную и кабинет бухгалтерии.
- Аппаратура защиты от акустической разведки «Соната АВ» модель 4Б;
- Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РЗ.1».
- Жалюзи на 8 окон.

Оценим количество компонентов и расстановку выбранных технических средств. Соната АВ-4Б содержит генераторы-акустоизлучатели СА-4Б и генераторы-вибровозбудители СВ-4Б. Согласно официальному сайту НПО, необходимое количество генераторов-вибровозбудителей СВ-4Б можно предварительно оценить из следующих норм:

- Стены – один на каждые 3–5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- Потолок, пол – один на каждые 15–25 м<sup>2</sup> перекрытия;
- Один на окно (при установке на оконный переплет);
- Один на дверь (при установке на верхнюю перекладину дверной коробки);
- Трубы систем ЦО – один на каждую вертикаль (отдельную трубу) вида коммуникаций.



Необходимое количество генераторов-акустоизлучателей СА-4Б можно предварительно оценить из следующих норм:

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

Итоговое количество требуемых технических средств для рассматриваемого объекта защиты и их расчетная стоимость представлены в таблице 6.

Таблица 6 – Оценка стоимости технических средств защиты

Наименование средства	Количество, у. е.	Цена за штуку, руб.	Общая стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	1	21 600	21 600
Генератор-вибровозбудитель СВ-4Б	72	7 440	535 680
Генератор-акустоизлучатель СА-4Б	16	7 440	119 040
Пульт управления «Соната-ДУ4.4»	1	7 680	7 680
Размыкатель слаботочной линии Соната-ВК4.2	1	6 000	6 000
Размыкатель линии Ethernet Соната-ВК4.3	1	6 000	6 000
Соната-РЗ.1	7	31 120	217 840
Жалюзи-blackout	13	1 005	13 065
Усиленная звукоизолирующая дверь	4	31 800	127 200

Итого			1 054 105
-------	--	--	-----------

План помещения с установленными средствами технической защиты представлен на рисунке 4.

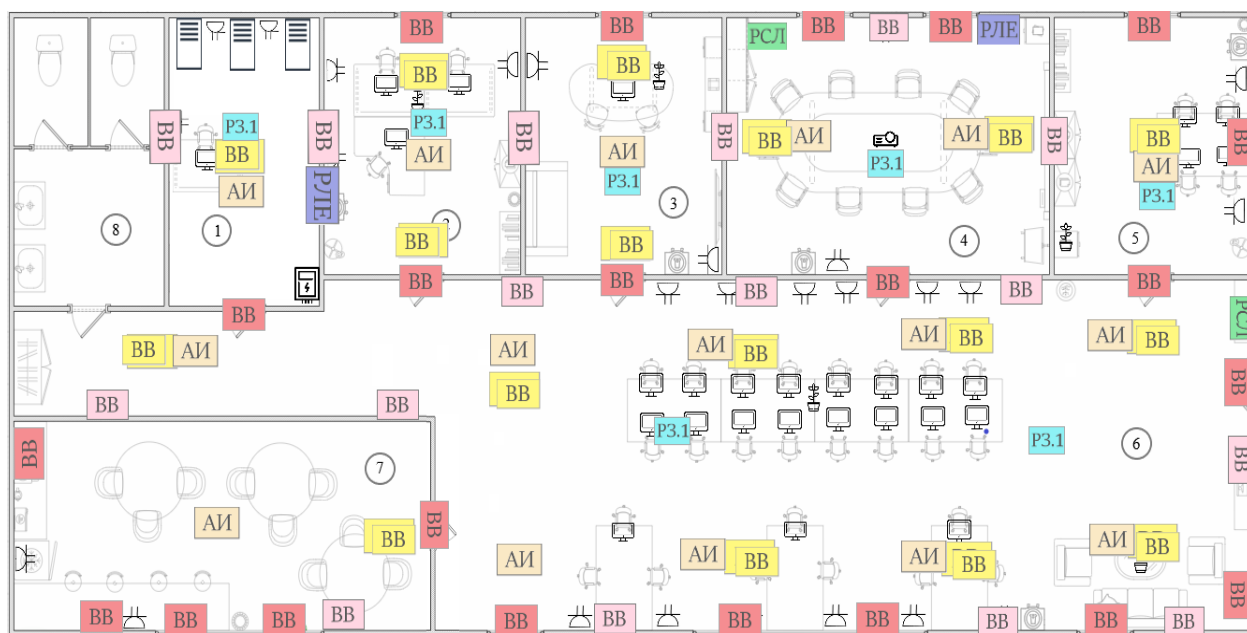







Рисунок 4 – План объекта с техническими СЗИ

Условные обозначения описаны в таблице 7.

Таблица 7 – Условные обозначения к рисунку 4.

Обозначение	Значение
АИ	Генератор-акустоизлучатель СА-4Б
ВВ	Генератор-вибровозбудитель СВ-4Б на окна, двери и радиаторы отопления
ВВ	Генератор-вибровозбудитель СВ-4Б на пол и потолок
ВВ	Генератор-вибровозбудитель СВ-4Б на стены

	Усиленная звукоизолирующая дверь
	Жалюзи-blackout
	Размыкатель линии Ethernet
	Размыкатель слаботочной линии
	Соната-РЗ.1

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был произведен теоретический обзор технических каналов утечки информации, анализ защищаемого предприятия, включая описание структуры предприятия, составление подробного плана помещений, описание информационных каналов.

Для выбора необходимых средств технической защиты информации был проведен анализ рынка существующих решений для противодействия рассматриваемым каналам утечки и выбраны наиболее подходящие для объекта решения. На основе выбранных средств был разработан план установки и произведен расчет финансовых затрат, которые указаны в разделе 5 данной работы.

В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному каналам. Затраты на обеспечение защиты составляют 1 054 105 руб., что можно считать достаточно оправданной суммой для объекта, который хранит и обрабатывает информацию, составляющую государственную тайну с грифом уровня «секретно».

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103203> (дата обращения: 01.11.2023). — Режим доступа: для авториз. пользователей
2. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург : НИУ ИТМО, 2013. — 148 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/43579> (дата обращения: 01.11.2023). — Режим доступа: для авториз. пользователей.
3. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва : ИНТУИТ, 2016. — 424 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100275> (дата обращения: 01.11.2023). — Режим доступа: для авториз. пользователей.
4. Каторин, Ю. Ф. Защита информации техническими средствами : учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. — Санкт-Петербург : НИУ ИТМО, 2012. — 416 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/40850> (дата обращения: 01.11.2023). — Режим доступа: для авториз. пользователей.
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам : Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. — Москва : Горячая линия-Телеком, 2005. — 416 с.