

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

**Факультет безопасности информационных технологий**

**Дисциплина:**


«Инженерно-технические средства защиты информации»

**КУРСОВАЯ РАБОТА**

«Проектировать системы защиты от утечки информации по различным источникам»

**Выполнил:**

Бульба Н.А., студент группы N34481



(подпись)

**Проверил:**

Попов И.Ю., к.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	Бульба Никита Александрович (фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34481
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении
Задание	Разработка комплекса инженерно-технической защиты информации в помещении

**Краткие методические указания**

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

**Содержание пояснительной записки**

1. Введение
2. Анализ организации
3. Оценка угроз
4. Анализ руководящих документов
5. Выбор средств защиты информации
6. Расположение средств защиты

**Рекомендуемая литература**

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

**Руководитель**

(Подпись, дата)

**Студент**



(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент** Бульба Никита Александрович  
(фамилия И.О.)

**Факультет** Безопасность Информационных Технологий

**Группа** N34481

**Направление (специальность)** 10.03.01 (Технологии защиты информации 2020)

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

**Дисциплина** Инженерно-технические средства защиты информации

**Наименование темы** Разработка комплекса инженерно-технической защиты информации в помещении

№ п/ п	Наименование этапа	Дата завершения		Оценка и подпись руководите ля
		Планируе мая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023	01.11.2023	
2	Анализ источников	01.11.2023	10.12.2023	
3	Написание отчета	15.11.2023	15.12.2023	
4	Представление выполненной курсовой работы	01.12.2023	19.12.23	

**Руководитель**

(Подпись, дата)

**Студент**



(Подпись, дата)

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	Бульба Никита Александрович (фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34481
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА  
(РАБОТЫ)**

Цель и задачи работы	Цель: провести мероприятия по организации защиты рассматриваемого помещения. Задачи: провести анализ защищаемого помещения; провести оценку каналов утечки информации; выбрать меры активной и пассивной защиты информации.
Характер работы	Конструирование
Содержание работы	7. Введение 8. Анализ организации 9. Оценка угроз 10. Анализ руководящих документов 11. Выбор средств защиты информации 12. Расположение средств защиты 13. Заключение 14. Список используемых источников
Выводы	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	 (Подпись, дата)
Студент	 (Подпись, дата)

## СОДЕРЖАНИЕ

Введение.....	6
1     Анализ организации .....	7
1.1    Общее описание.....	7
1.2    Информационные потоки.....	7
1.3    Защищаемое помещение .....	8
2     Оценка угроз.....	11
2.1    Оптический канал утечки.....	11
2.2    Акустический, виброакустический каналы .....	11
2.3    Электромагнитны канал.....	11
2.4    Закладные устройства .....	12
3     анализ руководящих документов.....	13
3.1    Перечень руководящих документов:.....	13
3.2    Требования к составу мер защиты .....	14
4     выбор средств защиты информации .....	16
4.1    Защита оптического канала.....	16
4.1    Защита акустического и виброакустического каналов .....	16
4.1    Защита электромагнитного канала .....	19
4.2    Защита от закладных устройств.....	22
5     расположение средств защиты.....	27
Заключение.....	28
Список использованных источников .....	29

## **ВВЕДЕНИЕ**

Цель работы – провести мероприятия по организации защиты рассматриваемого помещения.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ защищаемого помещения;
- провести оценку каналов утечки информации;
- выбрать меры активной и пассивной защиты информации.

# **1 АНАЛИЗ ОРГАНИЗАЦИИ**

## **1.1 Общее описание**

Наименование организации: "Инновационные Технологии и Безопасность (ИТБ)"

Область деятельности: специализированные разработки в области информационных технологий с акцентом на создание секретного программного обеспечения.

Тип взаимодействия: организация работает в формате B2B и B2G, предоставляя свои уникальные разработки и экспертизу в области информационной безопасности для других корпораций и государственных учреждений.

С увеличением объема государственных заказов руководство ООО "ИТБ" осознало важность надежной защиты информации, в особенности информации, которая относится к государственной тайне уровня "секретно". Работая в формате B2G, мы осознаем необходимость обеспечения офисного помещения техническими средствами защиты информации.

## **1.2 Информационные потоки**

Внутренняя структура организации "ИТБ" представляет собой слаженную систему, нацеленную на эффективную разработку секретного программного обеспечения (ПО) с учетом требующихся стандартов безопасности.

Разработка подразделена на небольшие группы, каждая из которых фокусируется на отдельных проектах.

Взаимодействие с заказчиками осуществляется через отдел продаж, где специалисты по связям обеспечивают эффективное взаимопонимание, снижая распространенность сведений конфиденциального характера.

Отдел HR занимается подбором и управлением персоналом, включая обеспечение безопасности информации при приеме и увольнении сотрудников.

Финансовый отдел занимается финансовым планированием и контролем, включая вопросы финансирования проектов.

Разработанная схема информационных потоков, представлен на рисунке 1, наглядно демонстрирует направление информации в организации. Красным выделен контур, по которому передаются сведения, составляющие государственную тайну, обеспечивая их защищенность и минимизацию доступа к ним внутри организации. Зеленым выделен периметр организации.

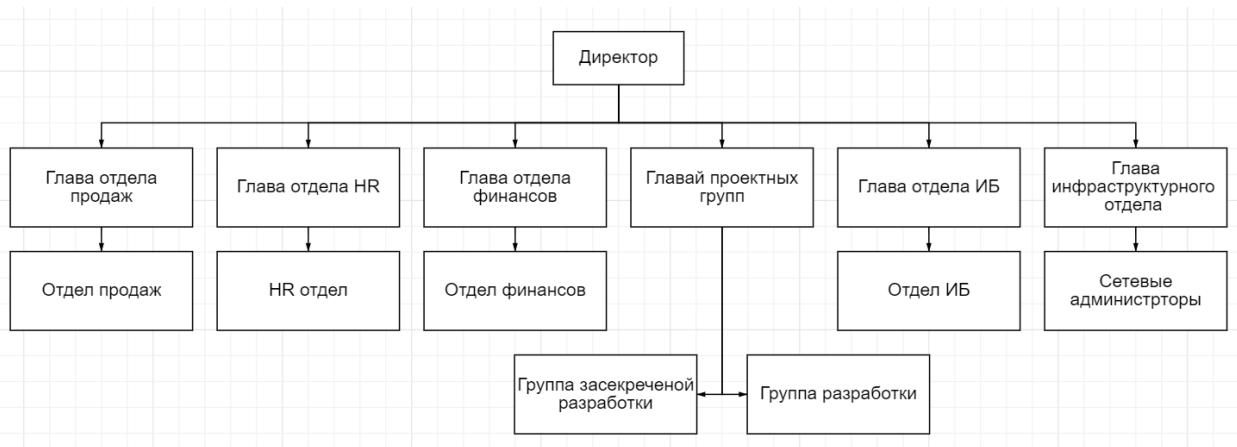


Рисунок 1 – Схема организационной структуры предприятия

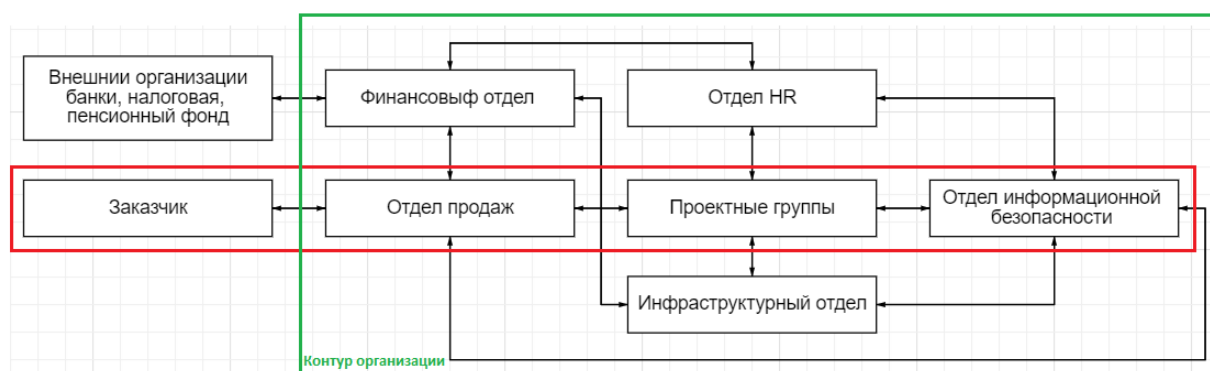


Рисунок 2 – Схема информационных потоков в организации

### 1.3 Защищаемое помещение

Офис нашей организации находится на 5 этаже в 7 этажном здании, сверху и снизу находятся другие арендуемые офисы, на северной стороне расположены окна, которые выходят на улицу, напротив расположены другие офисные здания, южная стена граничит с другими арендуемыми офисами в здании, а западная и восточные стены частично выходят на улицы, на которых расположены другие офисные здания и частично граничат с другими помещениями офисного здания. Стены здания и внутренние перегородки железобетонные с толщиной не менее 10 см.

Доступ к помещениям здания ограничен системой контроля и управления доступом. Доступ в здание и общие помещения здания имеют все сотрудники компаний, арендующих помещения в здании, доступ в офис нашей организации имеют только наши сотрудники.

Арендуемое помещение состоит из:

- два внутренних коридоров;
- складского помещения;



- серверной;
- зала для конференций (переговорная);
- open-space рабочая зона;
- зона для ведения закрытых разработок.

Работа со сведениями содержащими государственную тайну будет осуществляться в зоне для ведения закрытых разработок, также в зале для конференций (переговорной), будут происходить совещания, связанные с разработками данного типа.

План помещения предоставлен на рисунке 2, также на нем будут представлено описание элементы на плане, список комнат и их площадей приведены в таблице 1.

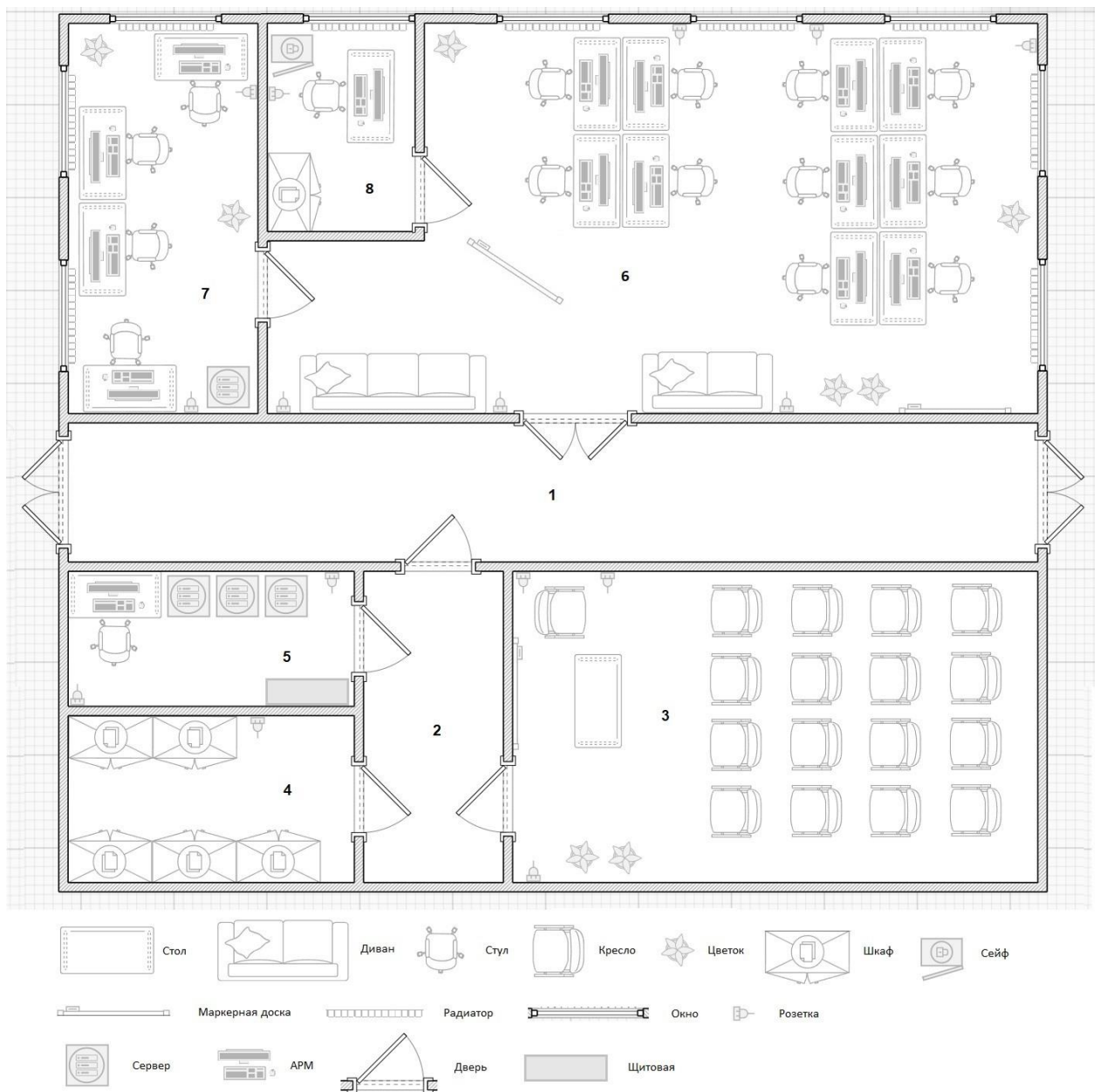


Рисунок 3 – План здания с описанием

Таблица 1 – Комнаты на плане

Номер на плане	Название	Площадь, м <sup>2</sup>
1	Коридор 1	15.62
2	Коридор 2	5.04
3	Зал для конференций (переговорная)	18.94
4	Склад	5.53
5	Серверная	4.48
6	Open-space рабочая зона	30.83
7	Зона для ведения закрытых разработок	8.57
8	Кабинет директора	3.60

Два коридора не содержат никакой мебели, только вентиляционные выходы.

В зале для конференций (переговорной) находятся кресла, маркерная доска, три розетки, два растения в горшках, стол и выход для вентиляции.

На складе расположены шкафы и полки с различными материалами и оборудованием.

В серверной находятся три серверные стойки, две розетки и одно АРМ.

Open-space зона содержит 11 рабочих мест, включая место руководителя с сейфом, шкаф для бумаг, 7 розеток, 6 окон, две маркерные доски, 4 растения в горшке, два дивана, входы для вентиляции и 6 радиаторов отопления.

В комнате для закрытых разработок, расположены: 4 рабочих места, 2 розетки, 3 окна и 3 радиатора, одна серверная стойка и два растения в горшках.

## **2 ОЦЕНКА УГРОЗ**

### **2.1 Оптический канал утечки**

Описание: оптический канал утечки представляет серьезную потенциальную угрозу для безопасности предприятия. С учетом расположения окон на стене офисного здания, существует реальная вероятность визуального наблюдения за внутренними процессами.

Оценка угроз: визуальное наблюдение включает в себя возможность фотографирования деятельности внутри помещения. Перехват визуальной информации может привести к утечке конфиденциальных данных, в том числе государственной тайны.

### **2.2 Акустический, виброакустический каналы**

Описание: акустический и виброакустический каналы представляют собой значительные потенциальные угрозы для безопасности предприятия, особенно в контексте проведения совещаний и ведения разработок в специальных помещениях.

Оценка угроз: угроза заключается в возможности записи и анализа звуковых данных изнутри помещения. Такие подслушивающие устройства могут стать источником утечки конфиденциальной информации, включая обсуждения проектов и другие чувствительные данные. В комнатах, где ведутся обсуждения секретной информации имеется вентиляция и радиаторы, возможно прослушивание через общую систему отопления или вентиляции, также из-за наличия окон с выходом на другие здания, появляется возможность съем информации через оконные стекла.

### **2.3 Электромагнитный канал**

Описание: электромагнитный канал представляет серьезную угрозу для безопасности предприятия, особенно при обработке и хранении конфиденциальной информации.

Оценка угроз: угроза включает в себя возможность перехвата электромагнитных излучений, которые могут содержать конфиденциальную информацию. Это может быть осуществлено с использованием специальных устройств, способных захватывать электромагнитные сигналы и преобразовывать их в читаемую форму. Также в каждой комнате у нас находятся розетки, отсюда появляется возможность считывать информацию через систему электропитания. Все работы с секретными данными и разработками осуществляются через компьютеры.

## **2.4   Закладные устройства**

Описание: закладные устройства, представляющие собой скрытные устройства для снятия информации, они могут стать серьезной угрозой для безопасности предприятия. Эти устройства могут использоваться для тайного сбора информации и неприметного наблюдения за деятельностью внутри помещений, создавая потенциальный риск утечки конфиденциальных данных.

Оценка угроз: угроза заключается в возможности установки закладных устройств для визуального и аудиослежения за сотрудниками и процессами внутри предприятия. Это может привести к компрометации конфиденциальной информации, а также к утечке государственной тайны. Эти устройства могут быть либо спрятаны где-то на территории офиса, либо быть замаскированными под другие устройства, розетки, лампы и т.п.

### **3 АНАЛИЗ РУКОВОДЯЩИХ ДОКУМЕНТОВ**

#### **3.1 Перечень руководящих документов:**

В процессе разработки комплекса мер по обеспечению безопасности информации в организации "Инновационные Технологии и Безопасность (ИТБ)", мы руководствуемся рядом ключевых руководящих документов, которые структурируют и определяют основные принципы работы в области информационной безопасности:

- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”: регламентирует основные нормы в области информационной безопасности и устанавливает требования к обработке и защите информации.
- Закон “О государственной тайне”: устанавливает общие принципы и порядок обращения с государственной тайной, формирует юридическую основу для работы с конфиденциальной информацией.
- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне": формирует перечень информации, считающейся государственной тайной, и определяет правила ее обращения.
- Постановление Правительства РФ от 15 апреля 1995 г. №333 “О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну”: устанавливает порядок лицензирования деятельности, связанной с государственной тайной, и контроля за соблюдением установленных правил.
- Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 29.10.2022) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне": регламентирует процедуры допуска персонала к работе с государственной тайной.
- Постановление Правительства РФ от 26 июня 1995 г. №608 “О сертификации средств защиты информации”: устанавливает процедуры и требования к сертификации средств защиты информации, обеспечивая их соответствие стандартам безопасности.
- ГОСТ Р ИСО/МЭК 27001-2021 “Системы менеджмента информационной безопасности. Требования”: устанавливает требования к системам менеджмента информационной безопасности.

- ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”: содержит рекомендации и указания по применению систем менеджмента информационной безопасности.

- ГОСТ Р ИСО/МЭК 27033-2011 “Безопасность сетей”: регулирует вопросы обеспечения безопасности в сетевых средах и управления информационными ресурсами.

- Приказ ФСТЭК России от 18 марта 2013 г. № 21 "Об утверждении Правил оказания услуг по технической защите конфиденциальной информации": определяет стандарты и правила для фирм, предоставляющих услуги по технической защите информации.

### **3.2 Требования к составу мер защиты**

Для обеспечения безопасности информации и соблюдения законодательных требований, предприятие "ИТБ" руководствуется следующими принципами:

- специализированные помещения: все помещения, где будет проводиться работа с государственной тайной, должны быть отдельными и оборудованы с учетом требований безопасности. Стены и перегородки между обычными и защищенными помещениями должны быть выполнены из бетона, железобетона или металла с минимальной толщиной стен не менее 10 см. Защищенные помещения должны иметь ограниченный доступ и обеспечиваться системой контроля и управления доступом;

- технические меры защиты: все используемые технические средства, включая аппаратуру, периферийные устройства и программное обеспечение, должны подлежать сертификации и соответствовать требованиям ФСТЭК. Применение технологий шифрования данных на всех этапах обработки, передачи и хранения конфиденциальной информации;

- организационные меры: регулярные обучения сотрудников по вопросам безопасности, включая правила работы с государственной тайной и выявление попыток социальной инженерии. Проведение обучающих-мероприятий для сотрудников с целью предотвращения утечек информации;

- стандарты и нормативы: соблюдение требований Закона "О государственной тайне", Федерального Закона №149 "Об информации, информационных технологиях и защите информации" и других документов, регулирующих работу с конфиденциальной информацией;

- физическая безопасность: обеспечение контроля и мониторинга физической безопасности с использованием систем видеонаблюдения и датчиков движения.

Регулярные инспекции и аудиты безопасности для выявления слабых мест в системе безопасности;

- аварийная готовность: оборудование всех режимных помещений аварийным освещением для обеспечения безопасной эвакуации персонала в случае чрезвычайных ситуаций;

- управление доступом: применение принципов минимальных привилегий при управлении доступом к информации. Контроль учетных записей и регулярное обновление списков лиц, имеющих доступ к государственной тайне.

## **4 ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

### **4.1 Защита оптического канала**

В качестве средств защиты от утечек по информационному каналу через окна, мы использовали плотные офисные рулонные шторы на окна, в таблице 2 представлена стоимость данного решения

Таблица 2 – Расчет стоимости штор и их установки

Наименование товара или услуги	Кол-во, шт.	Цена, руб.	Сумма, руб.
Шторы рулонные блекаут	4	1400	4200
Установка	1	2500	2500
Итог			8100

Также для защиты утечек по оптическому каналу через приоткрытые двери используется дверные заводчики. В таблице 3 представлен расчет стоимости.

Таблица 3 – Расчет стоимости доводчиков и их установки

Наименование товара или услуги	Кол-во, шт.	Цена, руб.	Сумма, руб.
Дверной доводчик APECS Vanger DC-120-SL 26414	12	1400	15400
Установка	1	2500	2500
Итог			19300

### **4.1 Защита акустического и виброакустического каналов**

Для обеспечения звукоизоляции комнат для закрытой разработки и переговорной, мы произведем шумоизолирующую отделку этих двух помещений. Все расчеты предоставлены в таблицах 4 и 5.

Таблица 4 – Расчет пассивной звукоизоляции

Наименование товара или услуги	Площадь, м <sup>2</sup>	Цена	Сумма, руб.
Звукоизоляция стен стоимость «под ключ» (работа + материалы)	82	4200 руб./кв.метр	344 400



Звукоизоляции потолка «под ключ» (работа + материалы)	28	4500 руб./кв.метр	126 000
Звукоизоляции пола «под ключ» (работа + материалы)	28	4000 руб./кв.метр	112 000
Итого			582 400

Таблица 5 – Звукоизолирующая дверь с установкой

Наименование товара или услуги	Кол-во, шт.	Цена, руб.	Сумма, руб.
Стальная звукоизолирующая дверь Experience 70 + установка	2	63 200	126 400
Итого			126 400

Для обеспечения защиты от утечек по виброакустическим каналам, мы сравнили несколько вариантов излучателей виброакустических помех (таблица 6)

Таблица 6 – Сравнение излучателей виброакустических помех

Наименование устройства	Характеристики	Стоимость, руб.
ЛГШ-404	<ul style="list-style-type: none"> <li>– генератор шума ЛГШ-404 (генераторный блок с 2 выходами);</li> <li>– вибровозбудители ЛВП-10 для установки на стекла, межкомнатные перегородки, трубы инженерных коммуникаций;</li> <li>– акустические излучатели ЛВП-2А, создающие маскирующие помехи в дверных проемах, вентиляционных воздуховодах и в прочих закрытых пространствах;</li> <li>– виброэкраны ЛИСТ-1 для установки на окна;</li> </ul>	35 100

	<ul style="list-style-type: none"> <li>– провода для подключения, крепежные элементы для монтажа</li> </ul>	
Буран	<ul style="list-style-type: none"> <li>– число помеховых каналов – три (виброакустических – 2, акустических – 1);</li> <li>– возможность подключения большого числа преобразователей - до 50 шт. (виброакустических – до 40 шт., акустических – до 10 шт.);</li> <li>– прецизионная система параллельного контроля линий подключения преобразователей;</li> <li>– вывод информации о состоянии работы системы на жидкокристаллический индикатор;</li> <li>– встроенная перестраиваемая система активной защиты информации от утечки по техническим каналам с программным управлением;</li> <li>– оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки;</li> <li>– возможность дистанционного включения системы по проводному каналу.</li> </ul>	35 000
Сонат АВ-4Б	<p>Предназначена для защиты помещений от утечки речевой информации по акустическому и виброакустическому каналам. В системе "Соната-АВ-4Б" генераторы шумового сигнала встроены непосредственно в каждый излучатель. Построение осуществляется по принципу "единый источник электропитания + генераторы-излучатели".</p> <p>Расширенная полоса частот генерируемого шумового сигнала позволяет использовать систему для защиты выделенных помещений до 1 категории включительно.</p>	44 200

Был сделан выбор в пользу ЛГШ-404, так как он больше всего подходит нам по сравнению цена, качество и функционал устройства.

#### 4.1 Защита электромагнитного канала

В таблице 7 указаны устройства для защиты от ПЭМИН, мы будем рассчитывать стоимость устройств на два помещения.

Таблица 7 – Сравнение средств активной защиты от ПЭМИН

Наименование устройства	Особенности	Стоимость, руб.
СОНАТА-РЗ.1	<ul style="list-style-type: none"><li>– комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления);</li><li>– наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений;</li><li>– возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0.01...100 МГц за счет применения опционально поставляемой дополнительной антенны;</li><li>– встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией;</li><li>– возможность удаленного управления изделием как в случае автономного использования (непосредственно Пульт-ДУ4.4), так и в случае использования в составе комплекса ТСЗИ;</li><li>– наличие счетчика наработки в режиме «Излучение».</li></ul>	33 120 * 2
SEL SP-44 Устройство защиты	<ul style="list-style-type: none"><li>– Цифровое автономное управление и контроль за настройками с защитой от несанкционированного доступа и выводом</li></ul>	24 000* 2

цепей электросети и заземления	<p>информации на встроенный жидкокристаллический экран.</p> <ul style="list-style-type: none"> <li>– Применение двух некоррелируемых формирователей шума для цепей «фаза»-«земля» и «ноль»-«земля» позволяет исключить возможность съёма информационного сигнала как для противофазной, так и для синфазной схем подключения.</li> <li>– Наличие независимых регуляторов уровня для низкочастотного и высокочастотного диапазонов позволяет оптимизировать спектр помехи по электромагнитной совместимости при сохранении достаточной эффективности маскировки.</li> <li>– Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания.</li> <li>– Наличие встроенного счётчика суммарного времени наработки генератора помех с регистрацией значений в защищённой энергонезависимой памяти.</li> <li>– Во время работы прибор постоянно осуществляет самотестирование и в случае неисправности выдаёт звуковой и световой сигнал.</li> </ul>	
ГЕНЕРАТОР ШУМА ГАММА ГШ-18	Изделие является техническим средством, предназначенным для маскировки информативных ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей и комплексов на объектах вычислительной техники путем формирования и излучения в окружающее пространство электромагнитного поля шума	29 400 * 2

	(ЭМПШ) и введения напряжения шума в цепи электропитания и заземления, токоведущие линии и коммуникации в диапазоне рабочих частот от 9 кГц до 6 ГГц.	
--	--	--

По результатам нашего сравнения мы выбрали Гамма-ГШ18, так как там есть большие возможности по настройкам.

Далее в таблице 8 будет приведено сравнение комплексов ПЭВМ, стоимость будет записана с учетом количества рабочих мест занятых для ведения закрытых разработок.

Таблица 8 – Сравнение ПЭВМ в защищенном исполнении

Наименование устройства	Характеристики	Стоимость, руб.
ПЭВМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ ЛИС-40.3	<ul style="list-style-type: none"> <li>– Intel® Core™ i3-10110U с графическим ядром Intel® UHD Graphics 620</li> <li>– «Windows» (10 Pro)</li> <li>– DDR4, 8 Гбайт</li> <li>– внутренний жесткий диск (3,5) 1 ТБ, 7200 об/мин SATA</li> <li>– Intel® UHD Graphics 620</li> </ul>	260 000 * 4
ПК В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ ЛИС-40НС	<ul style="list-style-type: none"> <li>– Intel® Core™ i5 / Intel® Core™ i7</li> <li>– «Windows 10 Pro, Astra Linux, без ОС</li> <li>– DDR4, 8 Гбайт</li> <li>– от 256 Гб, SSD / от 500 Гб, HDD</li> <li>– интегрированная: Intel® UHD Graphics 620</li> </ul>	125 000 * 4
ЭВМ ГАММА МБ-16-01	<ul style="list-style-type: none"> <li>– Intel Bay Trail J1900 2.4GHz</li> <li>– Free DOS</li> <li>– интегрированный Intel HD Graphics 4000, DirectX 11, OpenGL 3.0</li> <li>– 2x2Gb DDR3L 1066 МГц</li> <li>– 320Gb SATA</li> </ul>	280 000 * 4

Наиболее актуальными для выполнения наших задач ПЭВМ является ЛИС-40НС, мы будем использовать его.

## 4.2 Защита от закладных устройств

В таблице 9 показано сравнение средств обнаружение закладных устройств.

Таблица 9 – Сравнение средств для поиск закладных устройств

Наименование устройства	Особенности	Стоимость, руб.
Крона-М12	<ul style="list-style-type: none"><li>– Сверхвысокая скорость сканирования – до 25 ГГц/сек</li><li>– Малые габариты и вес – выполнено в едином компактном экранированном корпусе</li><li>– Встроенные аккумуляторы обеспечивают автономную работу до 4 часов</li><li>– Режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы</li><li>– Оснащается комплектом для обследования проводных линий и ИК диапазона</li><li>– Мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода</li><li>– Возможно подключение клавиатуры и мыши для стационарной работы</li></ul>	1 980 000
Крона-М6	<ul style="list-style-type: none"><li>– Сверхвысокая скорость сканирования – до 25 ГГц/сек</li><li>– Малые габариты и вес – выполнено в едином компактном экранированном корпусе</li><li>– Встроенные аккумуляторы обеспечивают автономную работу до 4 часов</li><li>– Режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы</li><li>– Оснащается комплектом для обследования проводных линий и ИК диапазона</li></ul>	1 360 000

	<ul style="list-style-type: none"> <li>– Мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода</li> <li>– Возможно подключение клавиатуры и мыши для стационарной работы</li> </ul>	
ST 600 ПИРАНЬЯ	<ul style="list-style-type: none"> <li>– РЕЖИМ «ДЕТЕКТОР МАГНИТНОГО ПОЛЯ» предназначен для поиска работающих подслушивающих устройств. Режим реализуется путем приема, преобразования и индикации электромагнитных сигналов, возникающих при работе электронных устройств. Для приема сигналов используется встроенная магнитная антенна.</li> <li>– Частотный диапазон антенны (0,04 - 30 кГц) позволяет обнаруживать устройства в экранированных корпусах.</li> <li>– РЕЖИМ «ТРАССОИСКАТЕЛЬ» предназначен для трассировки кабелей при поиске проводных подслушивающих устройств.</li> <li>– Режим реализуется путем подачи в проводную линию тестового сигнала (частотой 455 кГц, промодулированного двухтональным низкочастотным сигналом) и его приемом бесконтактным датчиком.</li> <li>– Тестовый сигнал формируется и подается в кабель генератором. Для компенсации затухания сигнала предусмотрена регулировка мощности генератора.</li> </ul>	195 000

Был выбран комплекс ST 600 ПИРАНЬЯ как наиболее многофункциональный и подходящий для нашей организации по характеристикам и цене.

Также мы сравнили устройства для подавления сигналов закладных устройств (таблица 10).

Таблица 10 – Сравнение средств подавления сигналов закладных устройств

<b>Наименование устройства</b>	<b>Особенности</b>	<b>Стоимость, руб.</b>
Блокиратор сотовой связи ЛГШ-719	Изделие предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандартах: IMT-MC-450, GSM900, E-GSM900, DSC/GSM-1800, DECT (ETS-300 175), IMT-900/1800/UMTS (3G), IMT-2000/UMTS, LTE-800 (4G), LTE-2600 и WiMAX (4G), Bluetooth, WiFi 2,4 ГГц	149 500
Блокиратор сотовой связи ЛГШ-715	Изделие предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандартах: IMT-MC-450, GSM-900, E-GSM900, DSC/GSM-1800, DECT (ETS-300 175), IMT-2000/UMTS (3G)	74 700
Блокиратор стандарта 4G (LTE-800) ЛГШ-705	Изделие предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандартах: LTE-800 (4G)	32 500
Блокиратор сотовой связи ЛГШ-725	Изделие предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандартах: IMT-MC-450, GSM-900, E-GSM900, DSC/GSM-1800, DECT (ETS-300 175), IMT-900/1800/UMTS (3G), IMT-2000/UMTS, LTE-800(4G), LTE-2600 и WiMAX (4G), Bluetooth, WiFi 2,4 ГГц и 5 ГГц	247 000

Мы выбрали устройство блокиратор сотовой связи ЛГШ-725, так как оно охватывал больше диапазонов чем остальные устройства, также мы можем контролировать мощность по каждому диапазону что важно в условиях работы вблизи помещений других организаций.



Также мы изучили устройства для подавления микрофонов (таблица 11).

Таблица 11 – Сравнение средств подавления микрофонов или диктофонов

Наименование устройства	Описание	Стоимость, руб.
БУБЕН-УЛЬТРА МАКС	<p>Прибор предназначен для подавления звукового сигнала при попытке записи на записывающие устройства, специальные технические средства, выносные микрофоны посредством генерации трех типов помех. А именно:</p> <ul style="list-style-type: none"> <li>- помехи в ультразвуковом диапазоне, воздействующей непосредственно на мембрану микрофона;</li> <li>- сложной звуковой помехи, воздействующей на АРУ записывающего устройства, тем самым увеличивая воздействие УЗП;</li> <li>- речеподобной помехи с периодической перестройкой во времени, для затруднения ее выделения из полезного сигнала.</li> </ul>	81 000 * 2
Супертонкий подавитель диктофонов и микрофонов SEL- 324V «Веер»	<p>Подавитель диктофонов и микрофонов SEL-324V «Веер» является эффективным устройством подавления микрофонов в диктофонах, мобильных телефонах и других средствах аудиозаписи путём излучения сложной структурированной помехи в ультразвуковом диапазоне, неслышимой для человеческого уха, но воздействующей своим звуковым давлением непосредственно на мембрану микрофона.</p>	87 000 * 2
Портативный подавитель диктофонов и микрофонов SEL- 310 «Комар»	<p>Несмотря на свою малогабаритность, SEL-310 «Комар» является мощным и самым эффективным в своем классе устройством подавления микрофонов в диктофонах, мобильных телефонах и других средствах аудиозаписи за счёт</p>	60 000 * 2

	направленного излучения сложной структурированной помехи в ультразвуковом диапазоне, неслышимой для человеческого уха, но воздействующей своим звуковым давлением непосредственно на мембрану микрофона.	
--	--	--

Был сделан выбор в пользу системы БУБЕН-УЛЬТРА МАКС, так как он наиболее подходит для нашей организации согласно функционалу который у него есть.

## 5 РАСПОЛОЖЕНИЕ СРЕДСТВ ЗАЩИТЫ

Далее на схеме будут изображен план размещения оборудования и условные обозначения устанавливаемого оборудования (Рисунок 3).

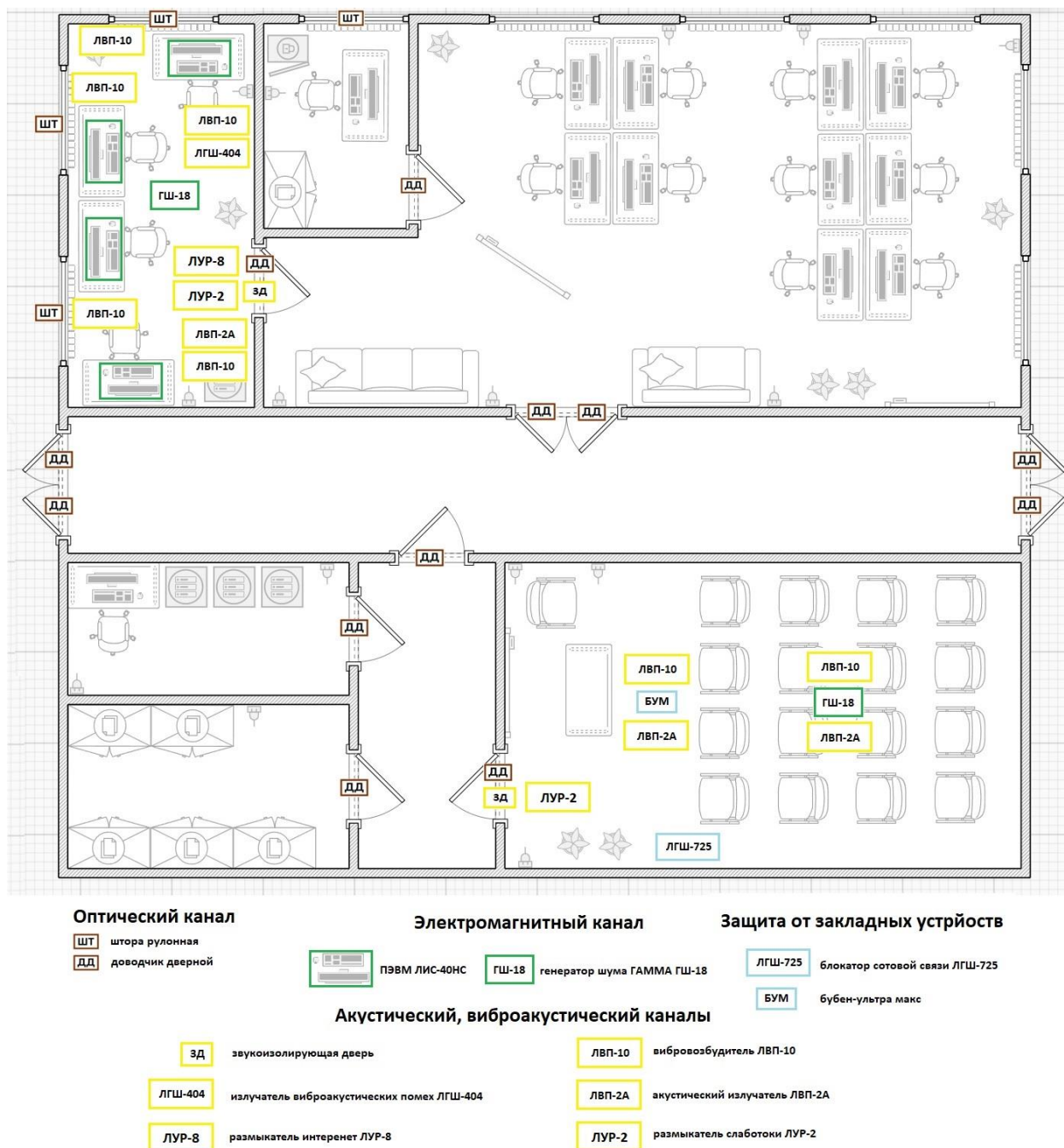


Рисунок 4 – План здания с размещением технических средств защиты информации

## **ЗАКЛЮЧЕНИЕ**

В ходе лабораторной работы мы изучили каналы утечки информации, произвели анализ потенциальных каналов утечки информации в данном нам помещении, также мы описали необходимые меры для защиты. Мы проанализировали рынок существующих технических средств и решений, после чего мы произвели план установки и произвели расчет стоимости предложенных активных и пассивных средств защиты информации.

В результате были произведены защитные меры по утечкам из различных каналов.

Итоговая стоимость защиты информации составила 1 934 100 рублей.

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. - 151 с. – экз.
2. 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