

**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”**

**Выполнил(а):**

Лейман В.В., студент группы N34511



(подпись)

**Проверил преподаватель:**

Попов И.Ю., доцент ФБИТ, к. т. н.

(подпись)

**Отметка о выполнении:**

Санкт-Петербург

2023

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Лейман В.В.
<b>Факультет</b>	Безопасности информационных технологий
<b>Группа</b>	N34511
<b>Направление (специальность)</b>	Информационная безопасность
<b>Руководитель</b>	Попов И.Ю., доцент ФБИТ, к.т.н. (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
<b>Задание</b>	Спроектировать инженерно-техническую системы защиты информации на предприятии

**Краткие методические указания**

**Содержание пояснительной записки**

Курсовая работа включает разделы:

1. Введение
2. Виды каналов утечки информации.
3. Обследование организации.
4. Перечень руководящих документов.
5. Разработка методики предотвращения утечек информации по физическим каналам связи
6. Заключение

**Рекомендуемая литература**

-

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

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

<b>Студент</b>	Лейман В.В.
<b>Факультет</b>	Безопасности информационных технологий
<b>Группа</b>	N34511
<b>Направление (специальность)</b>	Информационная безопасность
<b>Руководитель</b>	Попов И.Ю., доцент ФБИТ, к. т. н. (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
<b>Задание</b>	Спроектировать инженерно-техническую системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и под руководите
		Планируемая	Фактическая	
1	Заполнение задания на курс.работу	01.12.2023	01.12.2023	
2	Анализ собранных материалов	05.12.2023	05.12.2023	
3	Написание курсовой работы	14.11.2023	15.11.2023	
4	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	Лейман В.В.
Факультет	Безопасности информационных технологий
Группа	N34511
Направление (специальность)	Информационная безопасность
Руководитель	Попов И.Ю., доцент ФБИТ, к. т. н. (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Спроектировать инженерно-техническую системы защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы:**

Цель: спроектировать инженерно-техническую системы защиты информации организации “BLACK.OUT”

Задачи: проанализировать каналы утечек информации, провести исследование организации, проанализировать рынок инженерно-технических средств, разработать инженерно-техническую систему защиты информации.

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

**2. Характер работы**

- ☐ Расчет ☐ Конструирование  
☐ Моделирование ☒ Другое

**3. Содержание работы**

В работе представлен результат анализа рынка инженерно-технических средств защиты информации и на его основе разработана инженерно-техническая система защиты информации на предприятии.

**4. Выводы**

В результате выполнения курсовой работы было проведено обследование НПАО “BLACK.OUT” и разработана инженерно-техническая система защиты информации организации.

Руководитель

---

(Подпись, дата)

Студент



---

(Подпись, дата)

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	8
1 ВИДЫ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	9
1.1 Визуально-оптический канал связи.....	9
1.2 Акустический.....	9
1.3 Электромагнитный.....	11
1.4 Материально-вещественный.....	12
2 ОБСЛЕДОВАНИЕ ОРГАНИЗАЦИИ.....	13
3 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ.....	17
4 АНАЛИЗ РЫНКА.....	19
5 РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.....	31
ЗАКЛЮЧЕНИЕ.....	33
СПИСОК ЛИТЕРАТУРЫ.....	34

## **ВВЕДЕНИЕ**

В мире, где информация становится все более ценным активом, предотвращение утечек данных становится вопросом первостепенной важности. Каналы связи представляют собой критическую часть инфраструктуры, поддерживающей передачу и хранение конфиденциальной информации. Каналы связи играют ключевую роль в современных информационных системах, обеспечивая передачу данных между устройствами и сетями. Однако, несмотря на их важность, они могут представлять собой потенциальные точки уязвимости, через которые информация может быть неправомерно доступна третьим лицам. Утечка данных может иметь серьезные последствия, включая потерю репутации, финансов, времени и даже работников.

Для устранения таких ситуаций используются различные технические средства, которые не позволяют информации распространяться дальше заданной зоны. А для более стабильной защиты необходимо спроектировать инженерно-техническую систему для организации, чтобы предотвратить утечки информации.

# **1 ВИДЫ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Канал утечки информации – это совокупность источника информации, материального носителя (или среды распространения несущего эту информацию сигнала) и средства выделения информации из сигнала или носителя.

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

Классификация каналов утечки информации следующая (Рисунок 1):

1.      визуально-оптические;
2.      акустические;
3.      электромагнитные;
4.      материально-вещественные.

## **1.1 Визуально-оптический канал связи.**

Оптический канал утечки информации реализуется непосредственным восприятием глазом человека окружающей обстановки путем применения специальных технических средств, расширяющих возможности органа зрения по видению в условиях недостаточной освещенности, при удаленности объектов наблюдения и недостаточности углового разрешения. Это и обычное подглядывание из соседнего здания через бинокль, и регистрация излучения различных оптических датчиков в видимом или ИК-диапазоне, которое может быть модулировано полезной информацией. При этом очень часто осуществляют документирование зрительной информации с применением фотопленочных или электронных носителей. Наблюдение дает большой объем ценной информации.

## **1.2 Акустический.**

Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по телефону;
- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;
- приемника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Акустические каналы утечки информации могут быть следующих видов:

- прямой акустический - в прямых акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. В



качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический. Перехват акустической (речевой) информации из выделенных помещений по данному каналу может осуществляться: с использованием портативных устройств звукозаписи (диктофонов), скрытно установленных в выделенном помещении, с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной среде), скрытно установленных в выделенном помещении, с передачей информации по радиоканалу, оптическому каналу, электросети 220 В, телефонной линии, соединительным линиям ВТСС и специально проложенным кабелям, с использованием направленных микрофонов, размещенных в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных помещениях (непреднамеренное прослушивание);

- виброакустический - виброакустический канал состоит из тех же элементов, что и акустический: объект сигнала, среда распространения, агент, принимающий данные. Различие состоит в характеристиках среды. Это не воздух, а строительные и иные конструкции, при прохождении по которым акустический канал создает вибрацию, снимаемую при помощи лазерного луча и преобразованную в информацию;

- акустоэлектрический - акустоэлектрические технические каналы утечки информации возникают вследствие преобразования информативного сигнала из акустического в электрический за счет “микрофонного” эффекта в электрических элементах вспомогательных технических средств и систем. Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающим “микрофонным эффектом”, специальных высокочувствительных низкочастотных усилителей (пассивный акустоэлектрический канал);

- акустооптический - съем информации осуществляется с плоской поверхности, колеблющейся под действием акустической волны, лазерным лучом в ИК-диапазоне, что обеспечивает невидимость его невооруженным глазом. В качестве поверхности, на которую оказывает воздействие акустическая волна, используется внешнее стекло окна. Стекло облучается источником лазерного излучения с внешней стороны, например из окна соседнего дома. На поверхности соприкосновения лазерного луча со стеклом происходит модуляция лазерного луча акустическими сигналами, генерируемыми в помещении (речь, звуковые

колебания работающих технических систем). После отражения от стекла модулированный по амплитуде и фазе лазерный луч принимается приемником ИК-излучения, преобразуется в электрический сигнал и после соответствующей обработки преобразуется в акустический сигнал, несущий интересующую информацию;

- параметрический - в результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации часто называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а следовательно, к изменению частоты излучения генератора, то есть к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной ёмкости с воздушным диэлектриком в колебательных контурах гетеродинов.

### **1.3 Электромагнитный.**

Данный канал наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

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

- побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;
- побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
- побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения элементов ТСПИ.

В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

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

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

#### **1.4 Материально-вещественный.**

Материально-вещественные каналы - это каналы утечки информации, возникающие за счет неконтролируемого выхода за пределы контролируемой зоны различных материалов и веществ, в которых может содержаться конфиденциальная информация.

Особенность материально-вещественного канала утечки информации состоит в том, что его наличие позволяет получать секретные сведения, находясь за пределами предприятия. Для получения информации изучаются внешние признаки объектов, физические и химические свойства твердых, газообразных и жидких веществ, случайно попадающих в окружающую среду с территории производства.

## 2 ОБСЛЕДОВАНИЕ ОРГАНИЗАЦИИ

В первую очередь, перед разработкой системы защиты информации, было проведено обследование предприятия с целью выявления его структурной организации, обрабатываемой информации и информационных потоков.

Наименование организации: НПАО “BLACK.OUT”

Область деятельности: Аутсорсинг IT-специалистов, занимающихся тестированием в формате Red Team.

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

- сведения составляющие государственную тайну;
- информация конфиденциального характера:
  - персональные данные;
  - коммерческая тайна

Информационные потоки и структура организации представлена на рисунке 2.1.

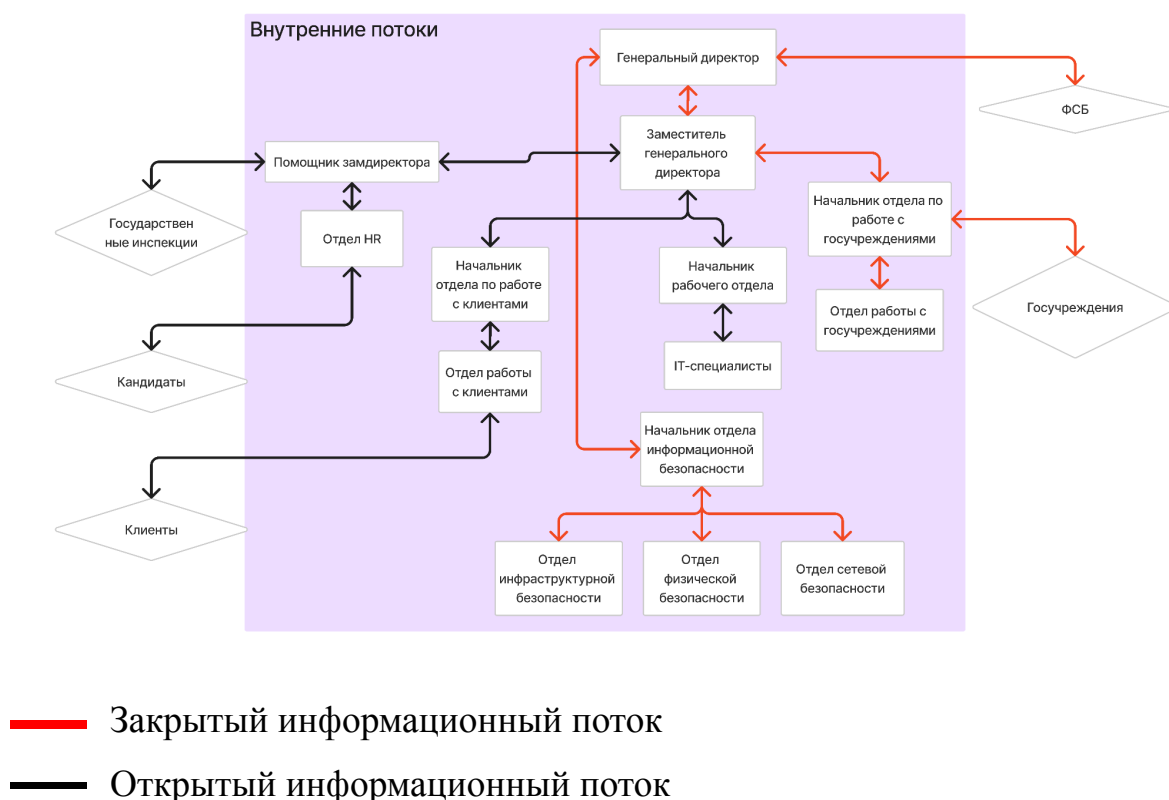


Рисунок 2.1 –Внутренние и внешние информационные

Прибыль, расходы, стоимость информационных активов:

- Прибыль: 70 000 000 рублей/мес
- Расходы:

- заработная плата сотрудников: 45 700 000 рублей/месяц;
- коммунальные услуги, интернет, обслуживание здания: 1 000 000 рублей/месяц;
- закупка и обслуживание оборудования и ПО: 5 000 000 рублей/месяц.
- Информационные активы:
  - сведения, составляющие государственную тайну: 500 000 000 рублей;
  - персональные данные сотрудников и клиентов: 200 000 000 рублей;
  - коммерческая тайна (структура, планы закупок, планы помещений и т.д.): 300 000 000 рублей.

Персонал организации: 55 человек.

План помещения:



Рисунок 2.2 – План помещения 1 этажа



Рисунок 2.3 – План помещения 2 этажа

Легенда:

1. Входное помещение.
2. Комната охраны.
3. Комната ожидания.
4. Коридор к санузлу.
5. Санузел женский.
6. Санузел мужской.
7. Кухня.
8. Опенспейс для работников.
9. Переговорная комната - обработка гостайны.
10. Комната отдыха.
11. Кабинет начальника отдела IT - обработка гостайны.
12. Кабинет HR
13. Кабинет отдела службы ИБ - обработка гостайны.
14. Коридор
15. Кабинет отдела по работе с клиентами
16. Переговорная комната - обработка гостайны.
17. Комната отдыха

18. Кабинет начальника отдела по работе с госучреждениями - обработка гостайны.
19. Отдел работы с госучреждениями - обработка гостайны.
20. Коридор к санузлу
21. Санузел мужской
22. Санузел женский
23. Спортивный зал
24. Кабинет директора - обработка гостайны.

Также необходимо привести перечень каналов для защиты. Они указаны в таблице 1.

Таблица 1 - перечень возможных каналов утечек информации

Канал	Источники	Возможная защита
Акустический	окна, двери, все твердые поверхности, стены, батареи	устройства акустического зашумления, устройства вибрационного зашумления, звукоизоляция
Электромагнитный	розетки, АРМы, ноутбуки	устройства электромагнитного зашумления
Визуально-оптический	окна, двери	жалюзи, шторы, рольставни, тонирующие пленки

### **3 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ**

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ “ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ”
2. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) "О коммерческой тайне".
3. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1.
4. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.
5. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
6. Постановление Правительства РФ от 15 апреля 1995 г. N 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".
7. Указ Президента РФ от 30 ноября 1995 г. N 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне".
8. Указ Президента Российской Федерации от 06.03.1997 г. № 188 “Об утверждении перечня сведений конфиденциального характера”.
9. Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам связи»(утв. Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51).

В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. № 188 “Об утверждении перечня сведений конфиденциального характера” организация НПАО “BLACK.OUT” обрабатывает:

- Сведения, раскрывающие методы, способы или средства защиты информации, содержащей сведения, составляющие государственную тайну, планируемые и (или) проводимые мероприятия по защите информации от несанкционированного доступа, иностранных технических разведок и утечки по техническим каналам, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.



- Сведения, раскрывающие методы, средства, организационные, технические или иные меры, направленные на обеспечение режима секретности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.

В соответствии с законом РФ "О государственной тайне" от 21.07.1993 N 5485-1. НПАО "BLACK.OUT" обрабатывает:

- сведения об организации и о фактическом состоянии защиты государственной тайны;
- о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

В соответствии с этими данными считаю оправданным создание инженерно-технической системы защиты информации на предприятии НПАО "BLACK.OUT"

## 4 АНАЛИЗ РЫНКА

Анализ рынка будет начат с анализа блокираторов беспроводной связи и блокираторов сотовой связи. Анализ представлен в таблице 2.

Таблица 2 - Блокираторы беспроводной связи, блокираторы сотовой связи

Название	Производитель	Описание	Цена
ЛГШ-725	Лаборатория ППШ	<p>Блокиратор является новой модификацией популярного генератора ЛГШ-719 с дополнительным подавлением сигналов WiFi на частоте 5 ГГц.</p> <p>Блокиратор сотовой связи ЛГШ-725 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах:</p> <ul style="list-style-type: none"> <li>- IMT-MC-450;</li> <li>- GSM900;</li> <li>- DSC/GSM1800, (DECT1800);</li> <li>- IMT-2000/UMTS (3G);</li> <li>- LTE 2600 (4G, WiMAX);</li> <li>- LTE 800 (4G);</li> <li>- Bluetooth;</li> <li>- WiFi 2.4 ГГц;</li> <li>- WiFi 5 ГГц.</li> </ul>	247 000 руб.
ЛГШ-719	Лаборатория ППШ	<p>Блокиратор сотовой связи ЛГШ-719 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах:</p> <ul style="list-style-type: none"> <li>- IMT-MC-450;</li> <li>- GSM900;</li> <li>- DSC/GSM1800, (DECT1800);</li> <li>- IMT-2000/UMTS (3G);</li> <li>- 4G-2600 (LTE, WiMAX);</li> <li>- 4G-800;</li> <li>- Bluetooth;</li> <li>- WiFi.</li> </ul>	149 500 руб.

Продолжение таблицы 2

ЛГШ-702	Лаборатория ППШ	Изделие ЛГШ-702 предназначено для блокирования (подавления) работы устройств, работающих в стандартах Bluetooth и WiFi. Изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, несанкционированной передачи данных, а также, для блокирования работы радиоисполнительных устройств, созданных с использованием стандартов Bluetooth и WiFi. Имеется сертификат ФСТЭК.	61 100 руб.
ЛГШ-703	Лаборатория ППШ	Изделие ЛГШ-703 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандарте IMT-2000/UMTS. Кроме того, изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, созданных на основе сотовых телефонов. В результате работы изделия происходит потеря сети оператора сотовой связи пользовательским терминалом и возвращение в нормальный режим работы после выключения изделия. Имеется сертификат ФСТЭК.	97 500 руб.
ЛГШ-701	Лаборатория ППШ	Изделие ЛГШ-701 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи работающих в стандартах: <ul style="list-style-type: none"> <li>- IMT-MC-450(NMT-450i);</li> <li>- GSM900;</li> <li>- E-GSM900</li> <li>- DSC/GSM1800</li> <li>- DECT1800</li> <li>- CDMA2000 1x</li> </ul>	97 500 руб.

		<ul style="list-style-type: none"> <li>- CDMA-800;</li> <li>- AMPS/N-AMPS/D-AMPS-800 /CDMA-800;</li> </ul>	
--	--	--	--

В качестве средства блокиратора для организации выбрано средство ЛГШ-701 производства Лаборатории ППШ, так как данное средство подавляет наибольшее количество стандартов сотовой связи, которые являются большую угрозу по сравнению с Wi-Fi или Bluetooth. Также у этого средства есть сертификата ФСТЭК.

Следующими средствами для анализа выбраны средства постановок акустических и виброакустических помех. Анализ представлен в таблице 3.

Таблица 3 - Средства постановок акустических и виброакустических помех

Название	Производитель	Описание	Цена
ЛГШ-304	Лаборатория ППШ	Предназначено для защиты акустической речевой информации, путем формирования акустических маскирующих шумовых помех. Диапазон рабочих частот - 175- 11200 Гц. Наличие сертификата ФСТЭК.	25 220 руб.
ЛГШ-301	Лаборатория ППШ	Генератор акустического шума ЛГШ-301 предназначен для защиты речевой информации от перехвата по прямому акустическому, виброакустическому и оптикоакустическому каналам. Изделие позволяет защищать речевую информацию, в обычном помещении, оборудованном сетью 220 В. Принцип действия ЛГШ-301 основан на генерации «белого шума» в акустическом диапазоне частот и, как следствие, повышении отношения акустическая помеха/речевой сигнал. Генератор защищает пространство объемом до 50 куб. м. Если Вы работаете в большом помещении, необходимо использовать несколько генераторов. Диапазон рабочих частот: 180-11300 Гц.	8 160 руб.

ЛГШ-404	Лаборатория ППШ	Средство акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными преобразователями. Диапазон рабочих частот 175 - 11200 Гц. Наличие сертификата ФСТЭК.	35 100 руб.
КАМЕРТ ОН-5	ЗАО "Зэт"	Камертон-5 – комплекс технических средств для защиты речевой информации от несанкционированного съема через виброакустические и акустические каналы. Использование данного оборудования гарантирует невозможность прослушки разговоров посредством лазерных и направленных микрофонов через окна, инженерные коммуникации, вентиляцию, межкомнатные перегородки, пр. Есть наличие сертификата ФСТЭК.	46 000 руб.
ВУАЛЬ	КБ "ЭЛАКС"	Защиты информации, обсуждаемой в служебных помещениях, от средств акустической речевой разведки. Диапазон рабочих частот - 100-11200 Гц. Вид помехи - "белый" шум. Число помеховых каналов - 3 Число каналов собственного зашумления - 1 Коэффициент корреляции каналов, не более - 0,1 Виды подключаемых к каждому каналу преобразователей: - акустические; - вибрационные. Наличие сертификата ФСТЭК.	44 730 руб.
Бубен-Уль тра	ИНФОСЕКЬЮР	Прибор предназначен для полного и (или) частичного подавления полезного звукового сигнала при попытке записи на мобильные или стационарные записывающие устройства, радио и проводные специальные технические средства, выносные микрофоны посредством	48 000 руб.

		<p>генерации двух типов помех. А именно:</p> <ul style="list-style-type: none"> <li>- помехи в ультразвуковом диапазоне, воздействующей непосредственно на мембрану микрофона;</li> <li>- акустический псевдослучайный сигнал типа «речевой хор», для затруднения ее выделения из полезного сигнала. Наличие сертификата ФСТЭК.</li> </ul>	
СОНАТА АВ-4Б	СОНАТА	<p>Соната-АВ” модель 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)" Благодаря этому построению проявляется высокая стойкость защиты информации.</p> <p>Имеет ряд преимуществ перед "классическим" подходом - "центральный генератор + электроакустические преобразователи":</p> <p>Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа</p> <p>Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы</p> <p>Улучшенная аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность:</p> <p>Создать систему автоматического контроля всех элементов</p> <p>Снизить время на конфигурирование и тестирование системы</p> <p>Изменить настройки генераторов и построить гибкую систему виброакустической защиты</p> <p>Наличие сертификата ФСТЭК.</p>	44 200 руб.

В качестве средства акустического и виброакустического средства постановки помех выбрана система СОНАТА АВ-4Б. Данная система имеет сертификат ФСТЭК, также имеется возможность ее установки в помещениях разной планировки и площади и возможность изменения количества включенных в систему излучателей без особых проблем. Имеется сертификат ФСТЭК.

Следующие средства для защиты - средства защиты сети 220/380 В. Анализ представлен в таблице 4.

Таблица 4 - средства защиты сети 220/380 В

Название	Производитель	Описание	Цена
ЛГШ-221	Лаборатория ПППШ	Сетевой генератор шума «ЛГШ-221» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок путем формирования маскирующих шумоподобных помех. Рабочий диапазон частот не менее 0,01 и не более 400 МГц Спектральная плотность напряжения шумового сигнала от 10 до 58 дБ. Наличие сертификата ФСТЭК.	36 400 руб.
ЛФС-10-1 Ф	Лаборатория ПППШ	Фильтр сетевой помехоподавляющий ЛФС-40-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц. Предельное значение тока, при котором допускается эксплуатация изделия 10 А. Наличие сертификата ФСТЭК.	47 060 руб.
ЛФС-200-3Ф	Лаборатория ПППШ	Фильтр сетевой помехоподавляющий «ЛФС-200-3Ф» предназначен для использования в целях защиты информации, обрабатываемой техническими средствами и системами и	377 000 руб.

		содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 380 В с частотой 50 Гц. Изделие «ЛФС-200-3Ф» является пассивным техническим средством защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. Предельное значение тока, при котором допускается эксплуатация изделия 200 А. Наличие сертификата ФСТЭК.	
--	--	---	--

В качестве средства защиты сети 220/380 В выбраны средства ЛГШ-221 и ЛФС-200-3Ф в качестве активного и пассивного соответственно.

Анализ средств для защиты от ПЭМИН представляет собой анализ средств пространственного зашумления. Анализ представлен в таблице 5.

Таблица 5 - средства пространственного зашумления

Название	Производитель	Описание	Цена
СОНАТА-ФС 10.1	СОНАТА	СЗИ помехоподавляющий сетевой фильтр "Соната-ФС10.1", предназначен для защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных наводок информативного сигнала на линии электропитания напряжением 220 В с частотой 50 Гц. Изделие представляет собой фильтр нижних частот, пропускающий сигнал на частоте напряжения линии электропитания и подавляющий высокочастотные сигналы и предназначено для подключения его к однофазной линии электропитания 220 В, 50 Гц по 3-проводной схеме. Изделие размещается внутри контролируемой зоны и подключается каскадно между источникам электропитания и	50 400 руб.



Продолжение таблицы 5

		потребителями. Наличие сертификата ФСТЭК.	
ЛГШ-501	Лаборатория ПППШ	Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-501» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех. Наличие сертификата ФСТЭК.	29 900 руб.
ЛГШ-503	Лаборатория ПППШ	Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-503» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех. Наличие сертификата ФСТЭК.	44 200 руб.
СОНАТА-РЗ	Соната	Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации. Диапазон частот 0,01 - 200 МГц.	97 200 руб.
ЛГШ-513	Лаборатория ПППШ	Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-513» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным	39 000 руб.

		доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех. Наличие сертификата ФСТЭК.	
--	--	---	--

В качестве средства пространственного зашумления выбрано средство ЛГШ-513.

Последним для анализа выбраны средства защиты линий связи. Анализ представлен в таблице 6.

Таблица 6 - средства защиты линий связи.

Название	Производитель	Описание	Цена
Размыкатель телефонной линии Соната-ВК4.1	СОНАТА	Прибор из линейки размыкателей слаботочных линий отечественного бренда Соната. Это оборудование предназначено для предотвращения утечки конфиденциальной информации по проводным телефонным сетям. Размыкатель заглушает акустические побочные сигналы, распространяющиеся по проводам. Прибор обеспечивает такую мощность затухания сигналов, которая гарантирует невозможность съема данных методами ВЧ-навязывания и электроакустических преобразований.	6 000 руб.
Размыкатель слаботочной линии Соната-ВК4.2	СОНАТА	Размыкатель слаботочных линий с напряжением не более 25В. Это оборудование внедряется в проводные линии системы оповещения или сигнализации. Цель его использования состоит в подавлении побочных сигналов, распространяющихся по проводам этих систем и потенциально содержащих конфиденциальные данные. Размыкатель Соната-ВК4.2 надежно блокирует этот канал утечки информации.	6 000 руб.
Размыкатель линии Ethernet Соната-ВК4.	СОНАТА	Принцип работы Соната-ВК4.3 достаточно простой. Кабели локальной сети Ethernet (витая пара) соединяются не напрямую, а через размыкатель.	6 000 руб.

Продолжение таблицы 6

3		Соната-ВК4.3 обеспечивает затухание всех побочных сигналов и наводок, которые потенциально могут содержать конфиденциальную информацию.	
Размыкатель сигнальных и линий оповещения Р-4С	ЗАО "Зэт"	Размыкатель Р-4С является элементом системы виброакустической защиты КАМЕРТОН-5 и предназначен для размыкания сигнальных линий и линий оповещения для обеспечения защиты акустической речевой информации от утечки за счёт акустоэлектрических преобразований.	7 000 руб.
Размыкатель телефонных линий Р-4Т	ЗАО "Зэт"	Это оборудование предназначено для предотвращения утечки конфиденциальной информации по проводным телефонным сетям. Размыкатель заглушает акустические побочные сигналы, распространяющиеся по проводам. Прибор обеспечивает такую мощность затухания сигналов, которая гарантирует невозможность съема данных методами ВЧ-навязывания и электроакустических преобразований.	7 000 руб.
Размыкатель локальной сети Р-8И	ЗАО "Зэт"	Размыкатель локальной сети Р-8И служит для размыкания локальной вычислительной сети, подключается разъемами RJ -45. Защита внешнего периметра сети от вредоносного воздействия со стороны сетей общего пользования. Создание отказоустойчивой VPN-сети между территориально распределенными сетями.	7 000 руб.
ЛУР 2	Лаборатория ППШ	Размыкатель слаботочных линий питания	5 590 руб.
ЛУР 4	Лаборатория ППШ	Размыкатель слаботочных линий Телефон	5 590 руб.
ЛУР 8	Лаборатория ППШ	Размыкатель слаботочных линий Ethernet	5 590 руб.

В качестве средств защиты линий связи выбраны: размыкатель слаботочной линии Соната-ВК4.2, размыкатель линии Ethernet Соната-ВК4.3. Их можно использовать в сочетании с система СОНАТА АВ-4Б, которая выбрана в качестве акустической и виброакустической защиты. Данные технические средства входят в состав данной системы, что позволит вести управление ещё легче. Размыкатель телефонной линии Соната-ВК4.1 не выбран в качестве инженерно-технического средства, так как в НПАО “BLACK.OUT” отсутствуют телефонные линии.

В качестве средств защиты визуально-оптического канала можно выбрать следующие средства:

- шторы на окна;
- жалюзи;
- тонированные пленки на стеклах;
- рольставни;
- доводчики на дверях.

Лучшим средством из этих я считаю жалюзи, рольставни и доводчики на дверях. Жалюзи не только перекрывают визуально-оптический канал, но и может использоваться в повседневной жизни сотрудников, например, закрытие от солнца. Рольставни можно использовать как средства против физического вмешательства и вандализма, лучше их использовать после закрытия организации, например ночью. Доводчики на дверях же предостерегают незакрытие дверей. Через щели, которые могут оставаться после того, как человек не закрыл дверь до конца можно подглядеть информацию, вследствие чего может произойти утечка информации.

В ходе анализа я выбрал следующие средства защиты:

Защита акустического и виброакустического канала: система СОНАТА АВ-4Б, что является средством активной защиты.

В качестве блокиратора связи: ЛГШ-701, что является средством активной защиты.

В качестве защиты сети 220/380 В: ЛГШ-221 и ЛФС-200-3Ф в качестве активного и пассивного соответственно.

В качестве средства пространственного шумления: ЛГШ-513, что является средством активной защиты.

В качестве средств защиты линий связи: размыкатель телефонной линии Соната-ВК4.1, размыкатель слаботочной линии Соната-ВК4.2, размыкатель линии Ethernet Соната-ВК4.3, что является средствами пассивной защиты.

В качестве средств защиты визуально-оптического канала: жалюзи, рольставни и доводчики на дверях, что является средствами пассивной защиты.

## 5 РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

На основе анализа планов помещения организации и рынка была разработана инженерно-техническая система защиты информации для организации НПАО “BLACK.OUT”. Состав и размещение средств представлены на рисунках 5.1 и 5.2.



Рисунок 5.1 - План первого этажа с инженерно-технической системой защиты информации

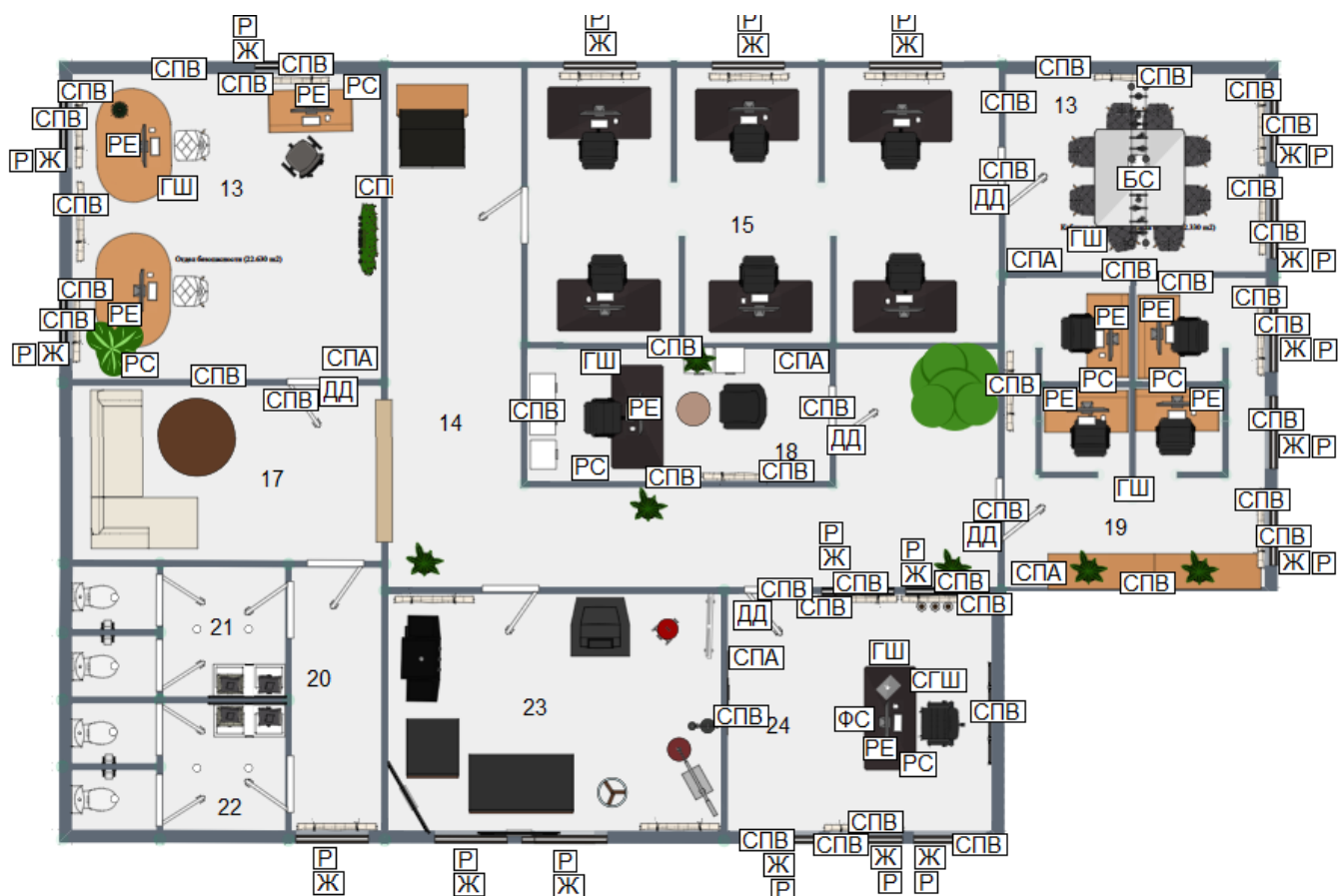


Рисунок 5.2 - План второго этажа с инженерно-технической системой защиты информации

Легенда:

СПА - Система постановки акустических помех;

СПВ - Система постановки виброакустических помех;

БС - Блокиратор связи;

ФС - Фильтр сетевой;

СГШ - Сетевой генератор шума;

ГШ - Генератор шума ПЭМИ;

РЕ - Размыкатель Ethernet;

РС - Размыкатель слаботочной линии;

Ж - Жалюзи;

Р - Рольставни;

ДД - Доводчик на дверь.

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы были выполнен анализ каналов утечки информации, обследование организации, проанализированы руководящие документы, проведён анализ рынка технических средств и разработана инженерно-техническая система НПАО “BLACK.OUT”.

Цель работы достигнута, все задачи выполнены.



## **СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Лаборатория ПППШ URL: <http://www.pps.ru/>.
2. Detector Systems URL: <https://detsys.ru/>.
3. Постановление Совета Министров – Правительства РФ "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам" от 15.09.1993 No 912-51.
4. Закон Российской Федерации "О государственной тайне" от 21.07.1993 No 5485-1.