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

**Факультет безопасности информационных технологий**

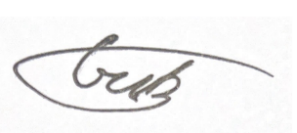
**Дисциплина:**

«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)

**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**  **руководителя** |
| **Планируемая** | **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** | 1. Введение 2. Анализ организации 3. Оценка угроз 4. Анализ руководящих документов 5. Выбор средств защиты информации 6. Расположение средств защиты 7. Заключение 8. 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](#_Toc153853253)

[1 Анализ организации 7](#_Toc153853254)

[1.1 Общее описание 7](#_Toc153853255)

[1.2 Информационные потоки 7](#_Toc153853256)

[1.3 Защищаемое помещение 8](#_Toc153853257)

[2 Оценка угроз 11](#_Toc153853258)

[2.1 Оптический канал утечки 11](#_Toc153853259)

[2.2 Акустический, виброакустический каналы 11](#_Toc153853260)

[2.3 Электромагнитны канал 11](#_Toc153853261)

[2.4 Закладные устройства 12](#_Toc153853262)

[3 анализ руководящих документов 13](#_Toc153853263)

[3.1 Перечень руководящих документов: 13](#_Toc153853264)

[3.2 Требования к составу мер защиты 14](#_Toc153853265)

[4 выбор средств защиты информации 16](#_Toc153853266)

[4.1 Защита оптического канала 16](#_Toc153853267)

[4.1 Защита акустического и виброакустического каналов 16](#_Toc153853268)

[4.1 Защита электромагнитного канала 19](#_Toc153853269)

[4.2 Защита от закладных устройств 22](#_Toc153853270)

[5 расположение средств защиты 27](#_Toc153853271)

[Заключение 28](#_Toc153853272)

[Список использованных источников 29](#_Toc153853273)

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.

# Анализ организации

## 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.

## Информационные потоки

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

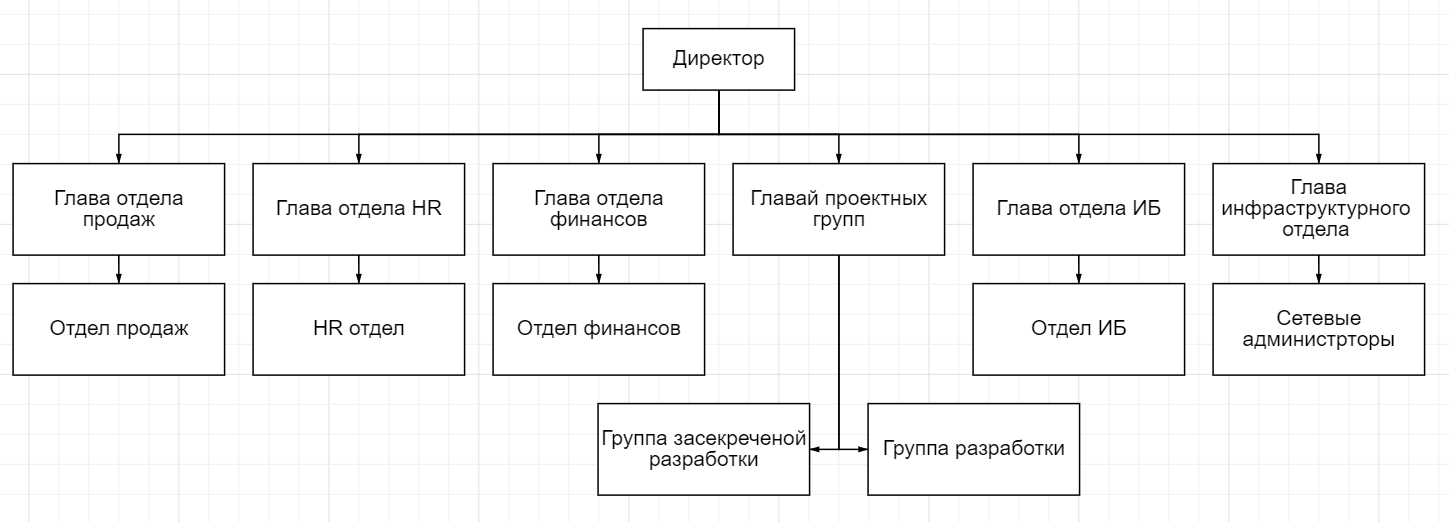
Разработка подразделена на небольшие группы, каждая из которых фокусируется на отдельных проектах.

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

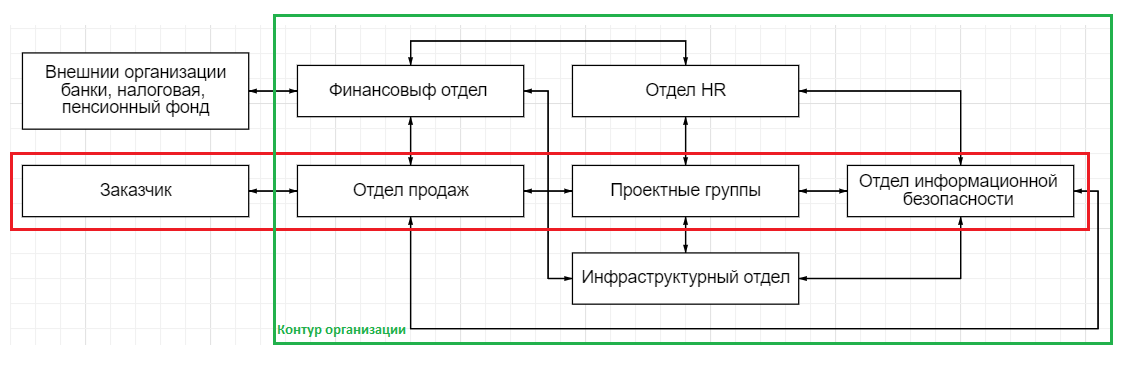
Отдел HR занимается подбором и управлением персоналом, включая обеспечение безопасности информации при приеме и увольнении сотрудников.

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.



1. Схема организационной структуры предприятия



1. Схема информационных потоков в организации

## 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.

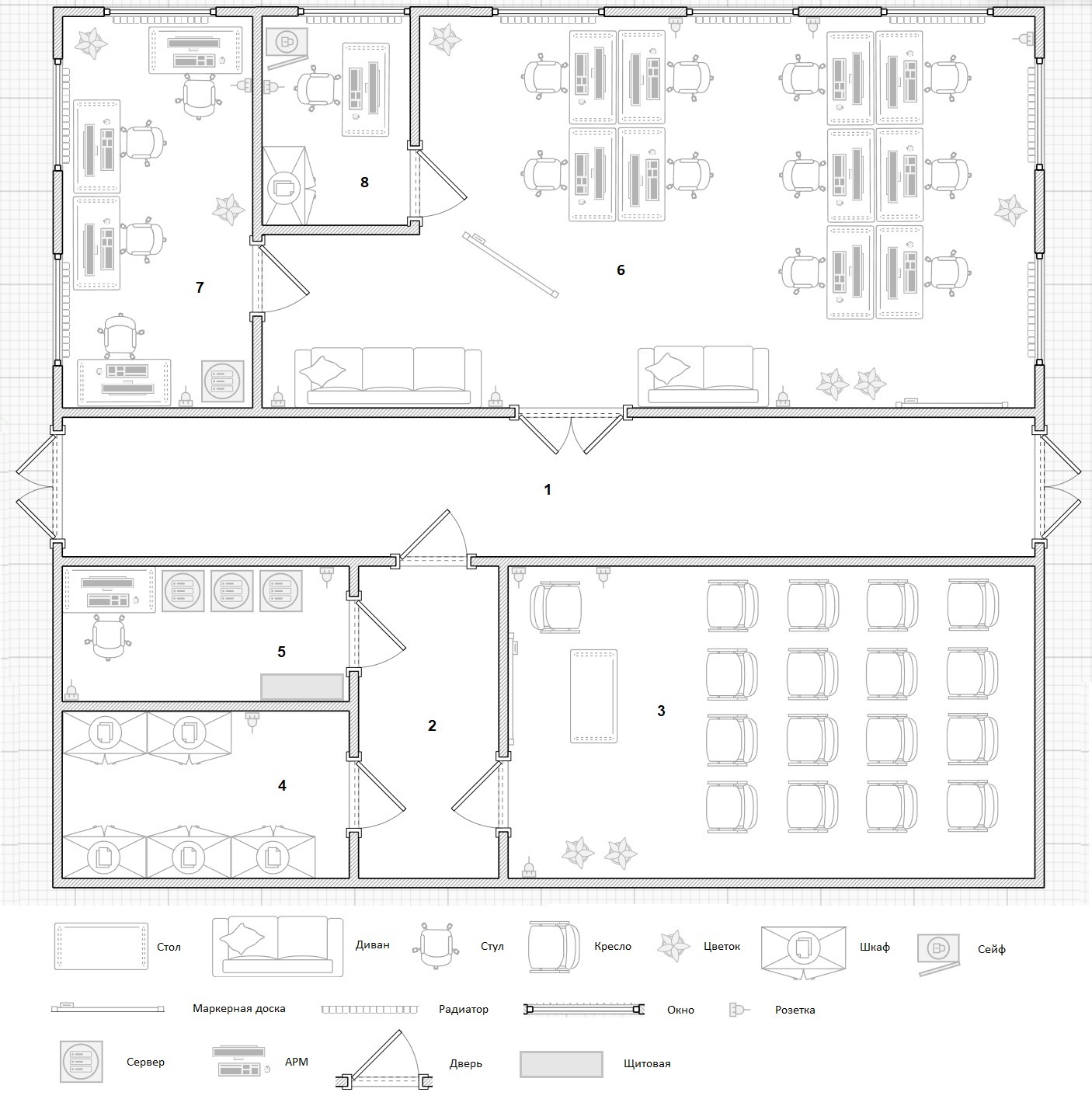
Доступ к помещениям здания ограничен системой контроля и управления доступом. Доступ в здание и общие помещения здания имеют все сотрудники компаний, арендующих помещения в здании, доступ в офис нашей организации имеют только наши сотрудники.

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.



1. План здания с описанием
2. Комнаты на плане

|  |  |  |
| --- | --- | --- |
| **Номер на плане** | **Название** | **Площадь, м2** |
| 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 кресал, 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.

# Оценка угроз

## 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.

## 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.

## Электромагнитны 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.

## 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.

# Анализ руководящих документов

## 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.

## 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.

# выбор средств защиты информации

## 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

1. 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.

1. 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 |

## Защита акустического и виброакустического каналов

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

1. Расчет пассивной звукоизоляции

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование товара или услуги** | **Площадь, м2** | **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 |
| Итог | | | 582 400 |

1. 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 |
| Итог | | | 126 400 |

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

1. Сравнение излучателей виброакустических помех

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Характеристики** | **Стоимость, руб.** |
| ЛГШ-404 | * генератор шума ЛГШ-404 (генераторный блок с 2 выходами); * вибровозбудители ЛВП-10 для установки на стекла, межкомнатные перегородки, трубы инженерных коммуникаций; * акустические излучатели ЛВП-2А, создающие маскирующие помехи в дверных проемах, вентиляционных воздуховодах и в прочих закрытых пространствах; * виброэкраны ЛИСТ-1 для установки на окна; * провода для подключения, крепежные элементы для монтажа | 35 100 |
| Буран | * число помеховых каналов – три (виброакустических – 2, акустических – 1); * возможность подключения большого числа преобразователей - до 50 шт. (виброакустических – до 40 шт., акустических – до 10 шт.); * прецизионная система параллельного контроля линий подключения преобразователей; * вывод информации о состоянии работы системы на жидкокристаллический индикатор; * встроенная перестраиваемая система активной защиты информации от утечки по техническим каналам с программным управлением; * оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки; * возможность дистанционного включения системы по проводному каналу. | 35 000 |
| Сонат АВ-4Б | 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". Расширенная полоса частот генерируемого шумового сигнала позволяет использовать систему для защиты выделенных помещений до 1 категории включительно. | 44 200 |

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

## Защита электромагнитного канала

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

1. Сравнение средств активной защиты от ПЭМИН

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Особенности** | **Стоимость, руб.** |
| СОНАТА-Р3.1 | * комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления); * наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений; * 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; * встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией; * возможность удаленного управления изделием как в случае автономного использования (непосредственно Пультом-ДУ4.4), так и в случае использования в составе комплекса ТСЗИ; * наличие счетчика наработки в режиме «Излучение». | 33 120 \* 2 |
| SEL SP-44 Устройство защиты цепей электросети и заземления | * Цифровое автономное управление и контроль за настройками с защитой от несанкционированного доступа и выводом информации на встроенный жидкокристаллический экран. * 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. * Наличие независимых регуляторов уровня для низкочастотного и высокочастотного диапазонов позволяет оптимизировать спектр помехи по электромагнитной совместимости при сохранении достаточной эффективности маскировки. * Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. * Наличие встроенного счётчика суммарного времени наработки генератора помех с регистрацией значений в защищённой энергонезависимой памяти. * Во время работы прибор постоянно осуществляет самотестирование и в случае неисправности выдаёт звуковой и световой сигнал. | 24 000\* 2 |
| 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 (ЭМПШ) и введения напряжения шума в цепи электропитания и заземления, токоведущие линии и коммуникации в диапазоне рабочих частот от 9 кГц до 6 ГГц. | 29 400 \* 2 |

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.

1. Сравнение ПЭВМ в защищенном исполнении

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Характеристики** | **Стоимость, руб.** |
| ПЭВМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ ЛИС-40.3 | * Intel® Core™ i3-10110U с графическим ядром Intel® UHD Graphics 620 * «Windows» (10 Pro) * DDR4, 8 Гбайт * внутренний жесткий диск (3,5) 1 TБ, 7200 об/мин SATA * Intel® UHD Graphics 620 | 260 000 \* 4 |
| ПК В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ ЛИС-40НС | * Intel® Core™ i5 / Intel® Core™ i7 * «Windows 10 Pro, Astra Linux, без ОС * DDR4, 8 Гбайт * от 256 Гб, SSD / от 500 Гб, HDD * интегрированная: Intel® UHD Graphics 620 | 125 000 \* 4 |
| ЭВМ ГАММА МБ-16-01 | * Intel Bay Trail J1900 2.4GHz * Free DOS * интегрированный Intel HD Graphics 4000, DirectX 11, OpenGL 3.0 * 2х2Gb DDR3L 1066 МГц * 320Gb SATA | 280 000 \* 4 |

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

## Защита от закладных устройств

В таблице 9 показано сравнение средств обнаружение закладных устройств.

1. Сравнение средств для поиск закладных устройств

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Особенности** | **Стоимость, руб.** |
| Крона-М12 | * Сверхвысокая скорость сканирования – до 25 ГГц/сек * Малые габариты и вес – выполнено в едином компактном экранированном корпусе * Встроенные аккумуляторы обеспечивают автономную работу до 4 часов * Режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы * Оснащается комплектом для обследования проводных линий и ИК диапазона * Мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода * Возможно подключение клавиатуры и мыши для стационарной работы | 1 980 000 |
| Крона-М6 | * Сверхвысокая скорость сканирования – до 25 ГГц/сек * Малые габариты и вес – выполнено в едином компактном экранированном корпусе * Встроенные аккумуляторы обеспечивают автономную работу до 4 часов * Режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы * Оснащается комплектом для обследования проводных линий и ИК диапазона * Мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода * Возможно подключение клавиатуры и мыши для стационарной работы | 1 360 000 |
| ST 600 ПИРАНЬЯ | * 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. * Частотный диапазон антенны (0,04 - 30 кГц) позволяет обнаруживать устройства в экранированных корпусах. * РЕЖИМ «ТРАССОИСКАТЕЛЬ» предназначен для трассировки кабелей при поиске проводных подслушивающих устройств. * Режим реализуется путем подачи в проводную линию тестового сигнала (частотой 455 кГц, промодулированного двухтональным низкочастотным сигналом) и его приемом бесконтактным датчиком. * Тестовый сигнал формируется и подается в кабель генератором. Для компенсации затухания сигнала предусмотрена регулировка мощности генератора. | 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).

1. Сравнение средств подавления сигналов закладных устройств

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Особенности** | **Стоимость, руб.** |
| 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 (ЕТS-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 (ЕТS-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 (ЕТS-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).

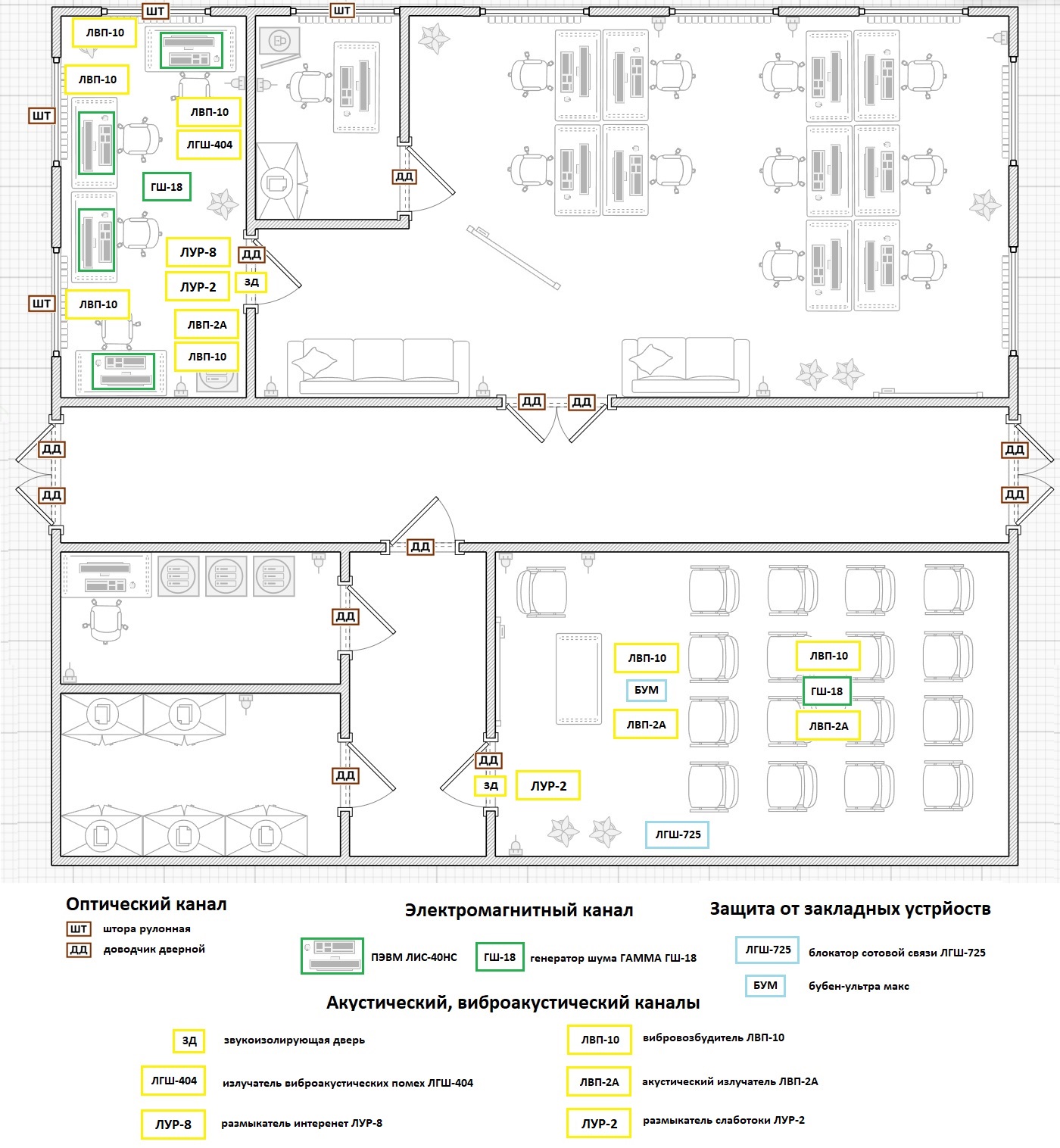
1. Сравнение средств подавления микрофонов или диктофонов

|  |  |  |
| --- | --- | --- |
| **Наименование устройства** | **Описание** | **Стоимость, руб.** |
| БУБЕН-УЛЬТРА МАКС | Прибор предназначен для подавления звукового сигнала при попытке записи на записывающие устройства, специальные технические средства, выносные микрофоны посредством генерации трех типов помех. А именно:  - помехи в ультразвуковом диапазоне, воздействующей непосредственно на мембрану микрофона;  - сложной звуковой помехи, воздействующей на АРУ записывающего устройства, тем самым увеличивая воздействие УЗП;  - речеподобной помехи с периодической перестройкой во времени, для затруднения ее выделения из полезного сигнала. | 81 000 \* 2 |
| Супертонкий подавитель диктофонов и микрофонов SEL-324V «Веер» | 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. | 87 000 \* 2 |
| Портативный подавитель диктофонов и микрофонов SEL-310 «Комар» | 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 направленного излучения сложной структурированной помехи в ультразвуковом диапазоне, неслышимой для человеческого уха, но воздействующей своим звуковым давлением непосредственно на мембрану микрофона. | 60 000 \* 2 |

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

# расположение средств защиты

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



1. 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 результаты были произведен 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