**Министерство науки и высшего образования Российской Федерации**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 защиты информации на предприятии

Вариант 51

**Выполнил:**

A black line drawing of a person's body

Description automatically generated

Назаров М. В., студент группы N34481

**Проверил преподаватель:**

Попов И. Ю., к.т.н.

**Отметка о выполнении:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Студент** | Назаров Максим Вячеславович | | | | | |  |
|  |  |  |  |  |  | (Фамилия И.О.) |  |
| **Факультет** |  | Безопасность информационных технологий | | | | | |
| **Группа** | N34481 | | |  |  |  |  |
| **Направление (специальность)** | | | | | | Информационная безопасность | |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | | | |
| **Наименование темы** | | | | Проектирование инженерно-технической системы защиты информации на предприятии | | | |
| **Задание** | Разработать систему инженерно-технической защиты информации на предприятии | | | | | | |
| **Краткие методические указания** | | | | | | | |
| 1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства | | | | | | | |
| защиты информации». | | | | | | | |
| 1. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, | | | | | | | |
| размещенных на коммуникационной площадке дисциплины. | | | | | | | |
| 1. Объект исследований курсовой работы ограничивается заданным помещением. | | | | | | | |
| **Содержание пояснительной записки** | | | | | | |  |
| 1. Введение. | | | | | | | |
| 1. Организационная структура предприятия. | | | | | | | |
| 1. Обоснование защиты информации. | | | | | | | |
| 1. Анализ защищаемых помещений. | | | | | | | |
| 1. Анализ рынка технических средств. | | | | | | | |
| 1. Описание расстановки технических средств. | | | | | | | |
| 1. Заключение. | | | | | | | |
| 1. Список литературы. | | | | | | | |
| **Рекомендуемая литература** | | | | | | | |
|  | | | | | | | |
| Руководитель | |  | | | | | |
|  |  |  |  |  |  |  | (Подпись, дата) |
| Студент | A black line drawing of a person's body  Description automatically generated | | | | | | 19.12.2023 |
|  |  |  |  |  |  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Назаров Максим Вячеславович | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасность информационных технологий | | | |
| **Группа** | N34481 | | |  |  |
| **Направление (специальность)** | | | | | Информационная безопасность |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | |
| **Наименование темы** | | | | Проектирование инженерно-технической системы защиты информации на предприятии | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование этапа** | **Дата завершения** | | **Оценка и подпись руководителя** |
| **Планируемая** | **Фактическая** |
| 1 | Разработка и утверждение задания и календарного плана на курсовую работу | 24.10.2023 | 24.10.2023 |  |
| 2 | Анализ теоретической составляющей | 20.11.2023 | 25.11.2023 |  |
| 3 | Разработка комплекса инженерно-технической защиты информации в заданном помещении | 29.11.2023 | 04.12.2023 |  |
| 4 | Представление выполненной курсовой работы | 19.12.2023 | 19.12.2023 |  |

|  |  |  |
| --- | --- | --- |
| Руководитель | |  |
|  |  | A black line drawing of a person's body  Description automatically generated(Подпись, дата) |
| Студент | 19.12.2023 | |
|  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Назаров Максим Вячеславович | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасность информационных технологий | | | |
| **Группа** | N34481 | | |  |  |
| **Направление (специальность)** | | | | | Информационная безопасность |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | |
| **Наименование темы** | | | | Проектирование инженерно-технической системы защиты информации на предприятии | |

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. **Цель и задачи работы**

Предложены студентом Сформулированы при участии студента

Определены руководителем

|  |
| --- |
| Целью работы является повышения уровня безопасности рассматриваемого помещения. Задачами является |
| проведение анализа безопасности помещения, оценка возможных каналов утечки информации, а также |
| определение мер по укреплению как пассивных, так и активных способов защиты информации. |

1. **Характер работы**

Расчет

Моделирование

Конструирование Другое

**Содержание работы**

|  |
| --- |
| 1. Введение. |
| 1. Организационная структура предприятия. |
| 1. Обоснование защиты информации. |
| 1. Анализ защищаемых помещений. |
| 1. Анализ рынка технических средств. |
| 1. Описание расстановки технических средств. |
| 1. Заключение. |
| 1. Список литературы. |

1. **Выводы**

|  |
| --- |
| В ходе исследования были выявлены универсальные стратегии для предотвращения утечек информации от |
| через технические каналы на предприятии. С учетом постоянно изменяющихся угроз кибер- и физической |
| безопасности подчеркивается необходимость применения современных методов для эффективной защиты |
| утечек данных. В данном контексте акцент делается не только на пассивных мерах безопасности, но и на |
| активных подходах. Важным фактором является осознание, что успешная защита требует не только |
| технологических инноваций, но также и формирования культуры безопасности внутри организации, |
| включая обучение сотрудников и повышение их ответственности. Таким образом, сбалансированный и |
| комплексный подход к вопросам безопасности остается ключевым элементом эффективных стратегий в |
| условиях современного информационного общества. |

|  |  |  |
| --- | --- | --- |
| Руководитель | |  |
|  |  | A black line drawing of a person's body  Description automatically generated(Подпись, дата) |
| Студент | 19.12.2023 | |
|  |  | (Подпись, дата) |

« » 20 г

**СОДЕРЖАНИЕ**

[Введение 7](#_Toc153850132)

[1 Организационная структура предприятия 8](#_Toc153850133)

[1.1 Анализ технических каналов утечки информации 8](#_Toc153850134)

[1.2 Информационные потоки 13](#_Toc153850135)

[1.3 Перечень руководящих документов 14](#_Toc153850136)

[1.4 Структура информационных потоков на предприятии 17](#_Toc153850137)

[2 Обоснование защиты информации 18](#_Toc153850138)

[3 Анализ защищаемых помещений 21](#_Toc153850139)

[3.1 Схема помещения 21](#_Toc153850140)

[3.2 Описание помещений 24](#_Toc153850141)

[3.3 Анализ возможных каналов утечки информации 26](#_Toc153850142)

[4 Анализ рынка технических средств 27](#_Toc153850143)

[4.1 Выбор средств защиты 27](#_Toc153850144)

[4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам 28](#_Toc153850145)

[4.3 Защита от утечки информации по (вибро-) акустическим каналам 31](#_Toc153850146)

[4.4 Защита от ПЭМИН 35](#_Toc153850147)

[4.5 Защита от утечек информации по оптическим каналам 38](#_Toc153850148)

[5 Описание расстановки технических средств 39](#_Toc153850149)

[Заключение 44](#_Toc153850150)

[Список использованных источников 45](#_Toc153850151)

# ВВЕДЕНИЕ

Средства защиты информации (СЗИ) предназначены для обеспечения безопасности данных в информационных системах, объединяющих хранимую в базах данных информацию, информационные технологии, ответственные за ее обработку, а также технические устройства. Использование таких средств направлено на предотвращение несанкционированного доступа к ресурсам и данным предприятия, что снижает риск утечек, утраты, искажения, уничтожения, копирования и блокирования информации. Эффективное разработка комплекса инженерно-технической защиты информации, классифицированной как государственная тайна уровня «совершенно секретно» на объекте информатизации, представлена в данной работе.

Объект защиты включает десять помещений и представляет офисное пространство предприятия, включая переговорную, кабинет директора, серверную, санузлы, кабинеты отдела разработки, главный холл, серверную и кухню. Структура работы включает пять глав, каждая из которых освещает важные аспекты обеспечения безопасности информации.

Первая глава посвящена анализу технических маршрутов возможной утечки информации. Вторая глава охватывает перечень управляющих документов, третья проводит анализ защищаемых помещений, учитывая риски утечек и необходимость технических средств обеспечения безопасности. Четвертая глава включает анализ рынка технических средств защиты информации, а последняя, пятая глава, посвящена разработке схемы размещения выбранных технических средств в защищаемых помещениях.

# ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

## **Анализ технических каналов утечки информации**

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

– разглашения конфиденциальной информации;

– ухода информации по различным, главным образом техническим, каналам;

– несанкционированного доступа к конфиденциальной информации различными способами.

Согласно теме курсовой работы, рассматриваться будет только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника.

Источниками сигнала могут быть:

– объект наблюдения, отражающий электромагнитные и акустические волны;

– объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;

– передатчик функционального канала связи;

– закладное устройство;

– источник опасного сигнала;

– источник акустических волн, модулированных информацией.

Информация от источника поступает на вход канала на языке источника, поэтому полученную информацию передатчик преобразует в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

– физические препятствия для субъектов и материальных тел;

– мера ослабления сигнала на единицу длины;

– частотная характеристика;

– вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

– выбор носителя с нужной получателю информацией;

– усиление принятого сигнала до значений, обеспечивающих съем информации;

– съем информации с носителя;

– преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.

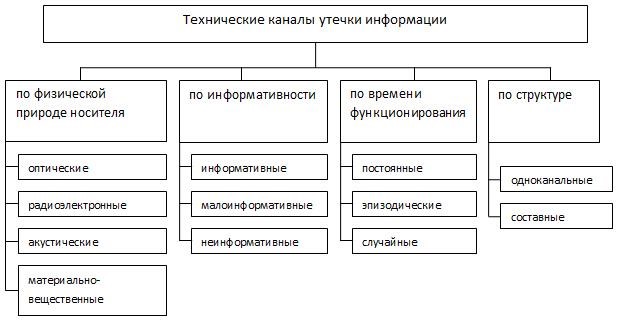


Рисунок 2 – Классификация технических каналов утечки информации

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Акустические ТКУИ в свою очередь делятся на акустоэлектрическом, виброакустическом и акустические.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействуют на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещение есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технические устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

## **Информационные потоки**

Информационный поток — это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления, анализа и контроля логистических операций. Они играют ключевую роль в функционировании предприятия, их правильное управление и защита существенны для обеспечения конфиденциальности, целостности и доступности информации. Они могут существовать в виде бумажных, электронных документов (носителей), звука, символов и сигналов.

Информационные потоки могут быть классифицированы по различным критериям. Согласно цели данной работы информационные потоки будут разделены на две основные категории: открытые и закрытые.

Открытые информационные потоки представляют собой те, которые доступны сотрудникам и другим заинтересованным сторонам в пределах предприятия без специальных ограничений. Они включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Примеры открытых информационных потоков включают в себя общие отчеты, обновления проектов и новости компании. Открытые информационные потоки способствуют эффективному внутреннему обмену информацией и содействуют открытости и прозрачности внутри организации.

Закрытые информационные потоки содержат конфиденциальную, чувствительную информацию, которая требует высокого уровня защиты. Эти потоки могут включать в себя финансовые данные, персональные записи, интеллектуальную собственность и другие данные, которые, если попадут в неправильные руки, могут нанести ущерб предприятию.

Защита закрытых информационных потоков включает в себя установление строгих политик доступа, шифрование данных, мониторинг активности и другие меры безопасности.

## **Перечень руководящих документов**

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

– «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212;

– «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;

– «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;

– «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108;

– «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594;

– «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;

– «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

– инструкция №0126–87;

– положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921–51;

– «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;

– «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333;

– «О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513;

– «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;

– «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;

– «О сертификации средств защиты информации» от 26 июня 1995 г, №608.

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

– СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;

– СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;

– методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;

– временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;

– временный порядок аттестации объектов информатизации по требованиям безопасности информации;

– руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;

– руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

– руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

– руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

– руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;

– руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования;

– руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей;

– руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Также, необходимо обратить внимания на законы Российской Федерации:

– «О государственной тайне» от 21 июля 1993 г. №5151–1;

– «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ;

– «О безопасности» от 5 марта 1992 г. №2446–1;

– «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1;

– «О связи» от 16 февраля 1995 г. №15-ФЗ;

– «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

## **Структура информационных потоков на предприятии**

На рисунке 3 розовым цветом обозначены открытые потоки, а зеленым цветом – закрытые потоки.

К информации, передающейся по открытым потокам, относятся бухгалтерская и финансовая отчетность, налоговые сведения.

К защищаемой информации, передающейся по закрытым потокам, относятся персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна и сведения о разрабатываемом программном продукте (программный код, назначение и т. д.).

A diagram of a company

Description automatically generated

Рисунок 3 – Схема информационных потоков на предприятии

# ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

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

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 сантиметров. Дверь устанавливается на металлический каркас;
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем эта­ же, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене;
4. Все режимные помещения оборудуются аварийным освещением;
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

Согласно Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники.

Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В» (таблица 1).

Таблица 1 – Классы защищенности автоматизированных систем

|  |  |  |
| --- | --- | --- |
| Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС) | 1А | В случае обработки секретной информации с грифом «особая важность» |
| 1Б | В случае обработки секретной информации с грифом не выше «совершенно секретно» |
| 1В | В случае обработки секретной информации с грифом не выше «секретно» |
| 1Г | АС, в которых циркулирует служебная информация |
| 1Д | АС, в которых циркулируют персональные данные |
| Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности) | 2А | Информация, составляющая гостайну |
| 2Б | Служебная тайна или персональные данные |

Продолжение таблицы 1

|  |  |  |
| --- | --- | --- |
| Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС) | 3А | Информация, составляющая гостайну |
| 3Б | Служебная тайна или персональные данные |

# АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

## **Схема помещения**

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке 4. В таблице 2 представлены описание обозначений, изображенных на плане.

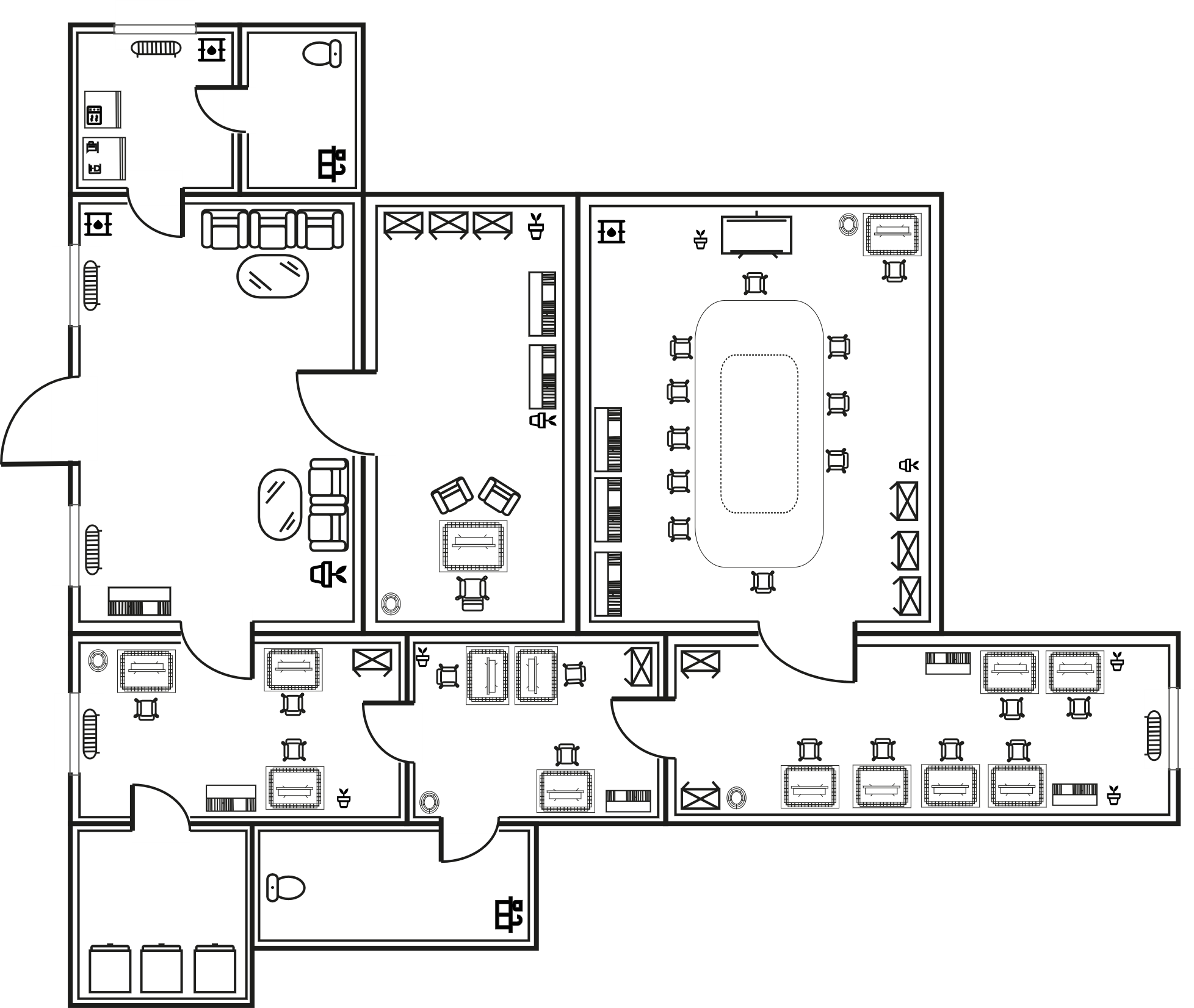


Рисунок 4 – План защищаемого помещения

Таблица 2 – Описание обозначений

|  |  |
| --- | --- |
| **Обозначение** | **Описание** |
|  | Интерактивнаядоска с проектором |
|  | Журнальный стол |
|  | Книжная полка |
|  | Комнатное растение |
|  | Компьютер |

Продолжение таблицы 2

|  |  |
| --- | --- |
| **Обозначение** | **Описание** |
|  | Компьютерный стол |
|  | Кофе машина |
|  | Кресло |
|  | Кулер для воды |
|  | Кухонный стол |
|  | Мусорное ведро для бумаги |
|  | Офисный стул |
|  | Радиатор отопления |
|  | Раковины |

Продолжение таблицы 2

|  |  |
| --- | --- |
| **Обозначение** | **Описание** |
|  | СВЧ-печь |
|  | Сервер |
|  | Стол переговоров |
|  | Стул руководителя |
|  | Унитаз |
|  | Чайник |
|  | Шкаф для документов |

## **Описание помещений**

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

– кабинет директора (20,8 м2);

– переговорная комната (25,2 м2);

– офис 1 (16,1 м2);

– офис 2 (13,3 м2);

– офис 3 (19,9 м2);

– серверная комната (8,4 м2);

– кухня (7,3 м2);

– главный холл (25,6 м2).

Кабинет директора включает в себя: один стул руководителя, два стула, один компьютерный стол, два книжных шкафа, три шкафа для документов, одно мусорное ведро для бумаги и два комнатных растения. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся одиннадцать стульев, один стол для переговоров, один компьютерный стол, один компьютер, три книжных шкафа, три шкафа для документов, одна интерактивная доска с проектором, один кулер для воды и два комнатных растения. Переговорная комната оснащена восьмью розетками.

Офис 1, офис 2 и офис 3 предназначены для сотрудников предприятия.

В офисе 1 стоят три стула, три компьютерных стола, три компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и одно комнатное растение. В данном помещении находятся шесть розеток.

В офисе 2 есть четыре стула, четыре компьютерных стола, четыре компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги и одно комнатное растение. Данное помещение оснащено восьмью розетками.

В офисе 3 находятся шесть стульев, шесть компьютерных столов, шесть компьютеров, два книжных шкаф, два шкафа для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и два комнатных растения. Офис 3 оснащен двенадцатью розетками.

В серверной комнате расположены три сервера. В данном помещении есть девять розеток.

В кухне есть кулер для воды и кухонный стол, на котором находятся одна кофемашина, одна микроволновая печь и один чайник, а также один радиатор отопления и одно окно. Данное помещение включает в себя пять розеток.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся два кресла (совмещенных), три кресла (совмещенных), два журнальных стола, один книжный шкаф, один кулер для воды, два радиатора отопления, одно комнатное растения и два окна.

Окна помещения выходят в закрытый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 13 см.

## **Анализ возможных каналов утечки информации**

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не перекрывается техническими средствами защиты.

# АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

## **4.1 Выбор средств защиты**

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 3. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 3 – Активная и пассивная защита информации

|  |  |  |  |
| --- | --- | --- | --- |
| **Каналы** | **Источники** | **Активная защита** | **Пассивная защита** |
| Электрический  Электромагнитный | Компьютеры, сервера, бытовая техника, розетки | Устройства электромагнитного зашумления | Защитные экраны и фильтры для сетей электропитания |

Продолжение таблицы 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Каналы** | **Источники** | **Активная защита** | **Пассивная защита** |
| Акустический  Электроакустический | Стены, двери, окна, электрические сигналы | Устройства акустического зашумления | Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений |
| Виброакустический | Стекла, стены и иные твердые поверхности | Устройства вибрационного зашумления | Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов |
| Визуально-оптический | Окна и стеклянные поверхности, двери | Жалюзи, бликующие устройства | Защитные экраны и фильтры для сетей электропитания |

## **Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам**

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 4.

Таблица 4 – Активная защита от утечек информации по электрическим каналам

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Соната-ФС 10.1 | 50 400 | Ток нагрузки – 10 А. Напряжение – номинальное напряжение 220 В. Частота – 50 Гц. Количество фаз – 1. Тип соединения – каскадно между источником электропитания и потребителями | Сертификат соответствия ФСТЭК России № 3885. Техническое средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок. Соответствует современным требованиям. Может устанавливаться в выделенных помещениях до 1-й категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. |

Продолжение таблицы 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| ФСП-1Ф-7А | 54 920 | Ток нагрузки – 10 А. Уровень шума/затухания – 80 дБ. Напряжение – 220 В. Частотный диапазон – 0,125 -1000 МГц. Количество фаз – 1. Тип соединения – подключение к однофазным цепям электропитания с заземляющим проводом. | Фильтр высокочастотных и импульсных помех, скачков напряжения на входе. Предназначен для встраивания в сеть с силой тока 7А, напряжением 220В, частотой 50Гц. Имеет небольшой вес и компактные размеры. Сертифицирован ФСТЭК, соответствует нормам ИСО и ГОСТ. |
| Генератор шума SEL SP-44 | 26 000 | Уровень шума затухания 12–90 дБ. Напряжение 220 В ± 10% 50 Гц. Диапазон частот 10 кГц – 400 МГц. Количество фаз – 1 с заземлением. | Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3–1 категорий. Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе. Возможность регулировки уровня ВЧ и НЧ шумов |

На основании анализа, проведенного в таблице 4, был выбран генератор шума SEL SP-44. Оптимальный вариант, так как устройство SEL SP-44 имеет сертификацию ФСТЭК и может проводить собственную диагностику, чтобы выявлять те или иные возникшие неисправности в работе. Также данный генератор шума издает звуковой сигнал при переходе в аварийный режим, что может уведомить пользователей в нужный момент.

## **Защита от утечки информации по (вибро-) акустическим каналам**

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б (таблица 5).

Таблица 5 – Активная защита от утечек информации по (вибро-)акустическим каналам

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Генератор шума ЛГШ-404 | 35 100 | Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В 12,5 ± 0,5. Электропитание сеть ~220 В/50 Гц. | Система сертифицирована ФСТЭК и может применяться в ВП 3 и 2 категорий. В состав системы входит генератор помех, виброэкраны и преобразователи (вибровозбудители и излучатели). Возможность подключения к генератору 40 преобразователей одновременно. Регулируемая мощность шумового сигнала. Счетчик времени наработки и световая индикация режима работы. |

Продолжение таблицы 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Соната АВ-4Б | 44 200 | Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В 12,5 ± 0,5. Электропитание сеть ~220 В/50 Гц. | Комплект состоит из блоков электропитания и управления, генераторов-акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров. |

Продолжение таблицы 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Генератор шума ЛГШ-402 | 18 200 | Электропитание – однофазная сеть переменного тока 187 В-242 В. Максимальное количество излучателей – 8 шт. Время непрерывной работы – круглосуточно. Диапазон воспроизводимого шумового сигнала – 175–11200 Гц. | Соответствует требованиям «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) – по 4 классу защиты. Соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными (не содержащими в своей конструкции индивидуальные задающие источники шума требующие электропитания) преобразователями. Оснащено визуальной системой индикации нормального режима работы |

Исходя из анализа, представленного в таблице 5, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов.

## **Защита от ПЭМИН**

Таблица 6 – Активная защита от ПЭМИН

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Генератор шума ПУЛЬСАР | 24 525 | Наличие регулировки уровня шума. Диапазон частот – 0,01–6000 МГц (для изделия, выпускаемого по ВСЦТ.464214.003 ТУ). Электропитание – выполнен в виде сетевого удлинителя с 5 розетками типа F. Мощность – 15 Вт. Режим работы – круглосуточно. | Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России) – по 2 классу защиты. Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук). Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа. |

Продолжение таблицы 6

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Генератор шума ЛГШ-501 | 29 900 | Присутствует регулировка уровня шума, диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Диапазон частот – 0,01–1800 МГц. Уровень шума – от -28 дБ(мкА/м\*√кГц) до 57 дБ(мкВ/м\*√кГц). Электропитание – однофазная сеть переменного тока 187 В-242 В. Мощность – не более 45 ВА. Режим работы – круглосуточно. | Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима. Оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним. |

Продолжение таблицы 6

|  |  |  |  |
| --- | --- | --- | --- |
| **Модель** | **Цена, руб.** | **Характеристики** | **Особенности** |
| Генератор шума ЛГШ-513 | 39 000 | Наличие регулировки уровня шума. Диапазон частот 10 кГц - 1800 МГц. Уровень шума от 0 до - 30 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А. | Сертификат ФСТЭК. Устройство соотвествует: типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений и типу «Б» - средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны |

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «ЛГШ-513». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

## **Защита от утечек информации по оптическим каналам**

Для прекращения функционирования оптического канала утечки информации можно применить следующие меры:

– шторы на окна;

– жалюзи;

– тонированные пленки на стеклах.

Шторы, как традиционное средство предотвращения скрытого наблюдения через окна кабинета, обладают недостатками, такими как существенное ухудшение естественной освещенности помещения и склонность к накоплению пыли.

Тонированные пленки на стеклах эффективны в исключении возможности наблюдения за объектами в кабинете. Однако они незначительно уменьшают освещенность помещения и могут легко выделять окна с повышенными требованиями к безопасности информации, что может противоречить принципам скрытности защиты. Рекомендуется использовать пленку на всех окнах, по крайней мере, на одном этаже, а предпочтительно – во всем здании.

Применение жалюзи на окнах представляет собой наиболее приемлемый вариант защиты, исключающий возможность наблюдения через окно и эффективно выполняющий функцию защиты от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь эффективны доводчики дверей, обеспечивающие плавное закрывание двери после ее открытия.

С целью предотвращения снимков экрана можно воспользоваться свободно распространяемым программным обеспечением ScreenWings, предназначенным для операционной системы Windows.

# ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

– сетевой генератор шума «SEL SP-44»;

– система виброакустической защиты «Соната АВ-4Б»;

– генератор шума «ЛГШ-513» от ПЭМИН

– жалюзи на семь окон;

– три усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

– стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;

– потолок, пол – один на каждые 15...25 м2 перекрытия;

– окна – один на окно (при установке на оконный переплет);

– двери – один на дверь (при установке на верхнюю перекладину дверной коробки);

– трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

– один на каждый вентиляционный канал или дверной тамбур;

– один на каждые 8...12 м3 надпотолочного пространства или других пустот.

В таблице 7 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 7 – Необходимое оборудование

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты** | **Цена, руб.** | **Количество, шт.** | **Итоговая стоимость** |
| Сетевой генератор шума «SEL SP-44» | 26 000 | 1 | 26 000 |
| Генератор шума «ЛГШ-513» | 39 000 | 1 | 39 000 |
| Блок электропитания и управления «Соната-ИП4.3» | 21 600 | 1 | 21 600 |
| Генератор-акустоизлучатель «Соната СА-4Б1» | 3 540 | 15 | 53 100 |
| Генератор-вибровозбудитель «Соната СА-4Б» | 7 440 | 59 | 438 960 |
| Рызмыкатель телефонной линии «Соната ВК4.1» | 6 000 | 2 | 12 000 |
| Рызмыкатель слаботочной линии «Соната ВК4.2» | 6 000 | 1 | 6 000 |
| Рызмыкатель линии «Ethernet» «Соната ВК4.1» | 6 000 | 1 | 6 000 |
| Пульт управления «Соната-ДУ 4.3» | 7 680 | 1 | 7 680 |
| Шторы-плиссе Blackout | 4 900 | 5 | 24 500 |
| Усиленные звукоизолирующие двери «Ultimatum Next ПВХ» | 83 619 | 3 | 250 857 |
| Итого |  |  | 885 697 |

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «SEL SP-44» и «ЛГШ-513» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 8 приведены описание обозначений устройств.

A blueprint of a building

Description automatically generated

Рисунок 5 – Схема расстановки устройств

Таблица 8 – Описание обозначений устройств

|  |  |  |
| --- | --- | --- |
| **Обозначение** | **Устройство** | **Количество, шт.** |
| A pink rectangle with black text  Description automatically generated | Блок электропитания и управления «Соната-ИП4.3» | 1 |
| A yellow rectangular sign with black text  Description automatically generated | Генератор-акустоизлучатель «Соната СА-4Б1» | 15 |
| A blue rectangle with black letters  Description automatically generated | Генератор-вибровозбудитель «Соната СВ-4Б» (стены) | 25 |

Продолжение таблицы 8

|  |  |  |
| --- | --- | --- |
| **Обозначение** | **Устройство** | **Количество, шт.** |
| A green rectangle with black text  Description automatically generated | Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол) | 16 |
| A yellow rectangle with black letters  Description automatically generated | Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи) | 18 |
| A purple rectangle with black letters  Description automatically generated | Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод) | 4 |
| A brown rectangle with white text  Description automatically generated | Размыкатель линии «Ethernet» «Соната-ВК4.3» | 1 |
| A brown rectangle with white text  Description automatically generated | Размыкатель слаботочной линии «Соната-ВК4.2» | 1 |
| A brown rectangle with white text  Description automatically generated | Размыкатель телефонной линии «Соната-ВК4.1» | 2 |
| A grey rectangular sign with black text  Description automatically generated | Сетевой генератор шума «SEL SP-44» | 1 |
| A black and white rectangle with a letter in it  Description automatically generated | Генератор шума “ЛГШ–513» | 1 |
| A black and white graph  Description automatically generated | Усиленные звукоизолирующие двери «Ultimatum Next ПВХ» | 3 |
| A grey rectangular object with a black stripe  Description automatically generated | Шторы-плиссе BlackOut | 5 |

# ЗАКЛЮЧЕНИЕ

При выполнении курсовой работы был проведен тщательный анализ как потоков информации, так и уровня безопасности помещений на предприятии. Обоснована неотложная необходимость обеспечения защиты информации, включающей государственную тайну уровня "совершенно секретно". Также проведен анализ рынка для выбора эффективных средств защиты, учитывая актуальные требования и тенденции.

На следующем этапе разработан план размещения технических средств защиты информации с детальными расчетами стоимости их внедрения. В результате проделанной работы создан комплексный план обеспечения безопасности помещения, который включает в себя меры по предотвращению утечек информации через разнообразные каналы, включая ПЭМИН, а также использование различных технологий, таких как электрические, акустоэлектрические, электромагнитные, акустические, виброакустические и оптические маршруты.

Цель данной работы – предоставление подробного и инновационного плана обеспечения защиты информации, который эффективно справится с современными вызовами и обеспечит высокий уровень безопасности помещения – была достигнута.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. – 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).