**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:**

Студент группы N34491

Басов Марк Игоревич

Изображение выглядит как спорт

Автоматически созданное описание\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Проверил преподаватель:**

Попов Илья Юрьевич, доцент ФБИТ, 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** | Басов М.И. | | | | | |  |
|  |  |  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасность информационных технологий | | | | | |
| **Группа** | N34491 | | |  |  |  |  |
| **Направление (специальность)** | | | | | | 10.03.01 (Технологии защиты информации) | |
| **Руководитель** | | Попов И. Ю., доцент, 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** | Цель: спроектировать инженерно-техническую систему защиту информации на предприятии. Задачи: 1. Выделить организационную структуру предприятия. | | | | | | |
| 2. Обосновать защиту информации. 3. Рассмотреть план предприятия. 4. Провести анализ рынка. | | | | | | | |
| 5. Разработать итоговый план предприятия. | | | | | | | |
| **Краткие методические указания** | | | | | | | |
|  | | | | | | | |
| **Содержание пояснительной записки** | | | | | | |  |
|  | | | | | | | |
| **Рекомендуемая литература** | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| Руководитель | |  | | | | | |
|  |  |  |  |  |  |  | (Подпись, дата) |
| Студент | Изображение выглядит как спорт  Автоматически созданное описание | | | | | | 13.12.2023 |
|  |  |  |  |  |  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Басов М.И. | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасность информационных технологий | | | |
| **Группа** | N34491 | | |  |  |
| **Направление (специальность)** | | | | | 10.03.01 (Технологии защиты информации) |
| **Руководитель** | | Попов И. Ю., доцент, 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 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование этапа** | **Дата завершения** | | **Оценка и подпись**  **руководителя** |
| **Планируемая** | **Фактическая** |
| 1 | Заполнение титульных листов и поиск источников | 15.11.2023 | 13.12.2023 |  |
| 2 | Анализ информации | 22.11.2023 | 15.11.2023 |  |
| 3 | Написание курсовой работы | 12.12.2023 | 15.12.2023 |  |
| 5 | Защита курсовой работы | 14.12.2023 | 19.12.2023 |  |

|  |  |  |
| --- | --- | --- |
| Руководитель | |  |
|  |  | (Подпись, дата) |
| Студент | Изображение выглядит как спорт  Автоматически созданное описание13.12.2023 | |
|  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Басов М.И. | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасность информационных технологий | | | |
| **Группа** | N34491 | | |  |  |
| **Направление (специальность)** | | | | | 10.03.01 (Технологии защиты информации) |
| **Руководитель** | | Попов И. Ю., доцент, 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 | |

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. **Цель и задачи работы**

Предложены студентом Сформулированы при участии студента

Определены руководителем

1. **Характер работы**

Расчет

Моделирование

Конструирование

Другое: Исследовательская работа

1. **Содержание работы**

В ходе работы я проанализировал рынок инженерно-технических средств защиты информации и разработал инженерно-техническую систему защиты информации предприятия.

1. **Выводы**

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему

защиты информации для предприятия «Сентри». Также я провел анализ рынка существующих

решений и разработал итоговый план предприятия.

|  |  |  |
| --- | --- | --- |
| Руководитель | |  |
|  |  | (Подпись, дата) |
| Студент | Изображение выглядит как спорт  Автоматически созданное описание13.12.2023 | |
|  |  | (Подпись, дата) |

«13» декабря 2023 г.

Содержание

[1. Введение 6](#_Toc153820573)

[2. Организационная структура предприятия 7](#_Toc153820574)

[3. Обоснование защиты информации 8](#_Toc153820575)

[4. Рассмотрение плана 16](#_Toc153820576)

[5. Анализ рынка 17](#_Toc153820577)

[6. Итоговый план предприятия 24](#_Toc153820578)

[7. Заключение 25](#_Toc153820579)

[8. Список использованных источников 26](#_Toc153820580)

# Введение

Целью моей курсовой работы является проектирование инженерно-технической системы защиты информации на предприятии.

Для достижения поставленной цели мне необходимо выполнить следующие задачи:

* выделить организационную структуру предприятия;
* обосновать защиту информации;
* рассмотреть план предприятия;
* провести анализ рынка существующих решений;
* разработать итоговый план предприятия.

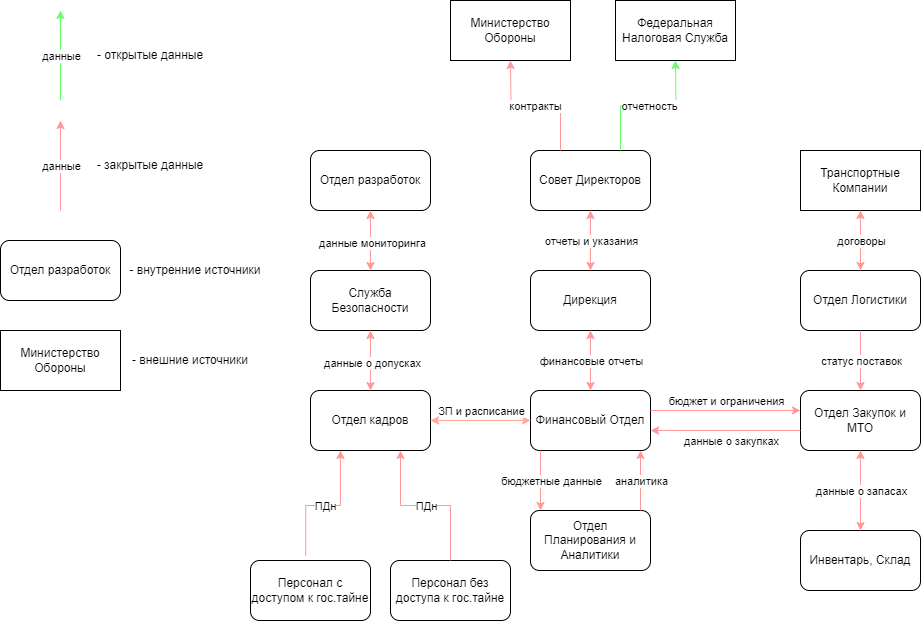
# Организационная структура предприятия

Для проектирования инженерно-технической системы защиты информации на предприятии мы должны провести анализ общих сведений данного предприятия.

Наименование организации: «Сентри»

Область деятельности: Разработка и производство зашифрованных коммуникационных систем для государственных структур и спецслужб. Организация «Сентри» специализируется на создании оборудования и программного обеспечения для обеспечения безопасного обмена информацией внутри страны и между союзными государствами.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа рассмотрены на Рисунке 1.



1. Основные информационные процессы и потоки в организации

# Обоснование защиты информации

Для обоснования необходимости защиты информации я провел анализ существующих Регламентов по защите данных (РПД). Учитывая, что мое предприятие занимается работой с государственной тайной, я также рассмотрел соответствующие документы, относящиеся к этой категории секретности.

**1. Законы Российской Федерации: «О государственной тайне» от 21 июля 1993 г. N 5485–1 (последняя редакция).**

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Государственную тайну составляют:

1. сведения в военной области:

* о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
* о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
* о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
* о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
* о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

1. сведения в области экономики, науки и техники:

* о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
* об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства
* об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
* о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

**Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайн**

Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

**Статья 30. Контроль за обеспечением защиты государственной тайны**

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

**2. Указы Президента Российской Федерации: «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.**

В соответствии со статьей 4 Закона Российской Федерации "О государственной тайне" постановляю:

1. Утвердить прилагаемый перечень сведений, отнесенных к государственной тайне.

2. Правительству Российской Федерации организовать работу по приведению действующих нормативных актов в соответствие с перечнем сведений, отнесенных к государственной тайне.

3. Настоящий Указ вступает в силу со дня его подписания.

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

В соответствии с Законом Российской Федерации "О государственной тайне" постановляю:

1. Образовать Межведомственную комиссию по защите государственной тайн

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

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:

Утвердить прилагаемый перечень сведений конфиденциального характера.

**3. Постановления Правительства Российской Федерации: 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.**

Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства РФ.

Защита осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путём проведения специальных работ, порядок организации и выполнения которых определяется Правительством РФ

Главными направлениями работ по защите информации являются:

* Обеспечение эффективного управления системой защиты информации
* Определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения
* Анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технически каналов утечки сведений, подлежащих защите
* Разработка организационно-технических мероприятий по защите информации и их реализация
* Организация и проведение контроля состояния защиты информации

Основными организационно-техническими мероприятиями по защите информации являются:

* Лицензирование деятельности предприятий в области защиты информации
* Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности
* Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам
* Введение территориальных, частотных, энергетически, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите
* Создание и применение информационных и автоматизированных систем управления в защищенном исполнении
* Разработка и внедрение технических решений и элементов защиты информации при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи
* Разработка средств защиты информации и контроля за её эффективностью (специального и общего применения) и их использование
* Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи

**«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.**

В соответствии с Законом Российской Федерации "О государственной тайне" и в целях установления порядка допуска предприятий, учреждений и организаций к 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, Правительство Российской Федерации постановляет:

1. Утвердить 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 (прилагается).

3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

4. Установить, что предприятия, учреждения и организации, допущенные к моменту принятия настоящего постановления к работам, связанным с использованием сведений, составляющих государственную тайну, могут осуществлять эти работы в течение 1995 года.

7. Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются - руководители предприятий), и при выполнении следующих условий:

* соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
* наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
* наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

**«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.**

В связи с созданием в Министерстве обороны Российской Федерации системы сертификации средств защиты информации, предусмотренной постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (Собрание законодательства Российской Федерации, 1995, N 27, ст. 2579), Правительство Российской Федерации постановляет :

Дополнить абзац третий пункта 2, абзацы второй и пятый пункта 10 Положения 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, утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 г. N 333 (Собрание законодательства Российской Федерации, 1995, N 17, ст. 1540; 1996, N 18, ст. 2142), после слов: "Служба внешней разведки Российской Федерации" словами: "Министерство обороны Российской Федерации".

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

1. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

2. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

3. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.

4. К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

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

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

В соответствии с Законами Российской Федерации "О государственной тайне" и "О сертификации продукции и услуг" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение о сертификации средств защиты информации.

2. Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Федеральной службе безопасности Российской Федерации и Министерству обороны Российской Федерации в пределах определенной законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующие положения о системах сертификации, перечни средств защиты информации, подлежащих сертификации в конкретной системе сертификации, а также по согласованию с Министерством финансов Российской Федерации порядок оплаты работ по сертификации средств защиты информации.

1. Настоящее Положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

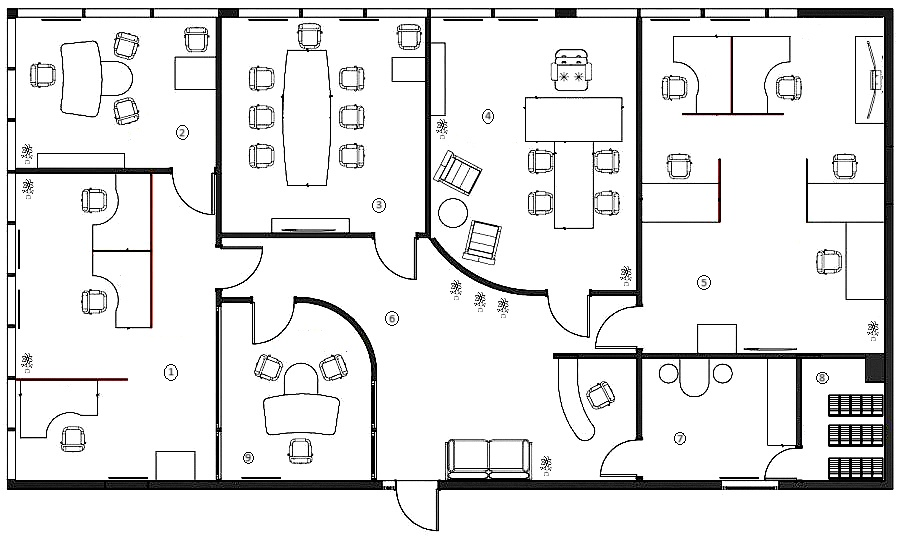
Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации).

Системы сертификации создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются – федеральные органы по сертификации).

# 4. Рассмотрение плана

В данном разделе я разработал план предприятия. План представлен на Рисунке 2.



1. План предприятия

Перечень комнат:

1. Финансовый Отдел
2. Кабинет второго менеджера
3. Переговорная
4. Кабинет руководителей
5. Отдел разработок
6. Коридор
7. Кухня (зона со столом и кофемашиной
8. Серверная
9. Кабинет главного менеджера

# 5. Анализ рынка

В данном разделе я проанализировал текущий рынок существующих решений по инженерно-технической защите информации, а также выбрал и описал наиболее подходящие решения.

1. Акустическое зашумление:

Акустическая система помех разработана с целью предоставления защиты от несанкционированного съема информации с использованием воздушной среды помещения в качестве канала передачи данных. Эта система направлена на противодействие специальным устройствам, таким как микрофоны и диктофоны, которые могут быть использованы для незаконного сбора акустической информации.

1. Виброакустическое зашумление:

Система внесения виброакустических помех создана с целью предотвращения несанкционированного сбора информации, при котором в качестве канала передачи данных используются ограждающие конструкции помещения. Это включает в себя следующие специальные средства:

* Электронные или акустические стетоскопы, предназначенные для прослушивания звуков, передающихся через потолки, полы и стены.
* Проводные или радиомикрофоны, установленные на ограждающих конструкциях помещения или на водопроводных и отопительных трубопроводах.
* Лазерные или микроволновые системы, которые могут использоваться для съема информации через оконные проемы помещений.

1. Защита электросети:

Сети переменного тока (220 В) представляют двойную угрозу безопасности информации. Это может быть утечка акустической информации через сеть переменного тока, а также риск утечки информации из устройств оргтехники.

Существуют пассивные и активные методы защиты сети переменного тока (220 В) от несанкционированного сбора информации.

* Пассивная защита сети 220 В включает использование сетевых помехоподавляющих фильтров. Эти фильтры предотвращают прохождение информативных сигналов, генерируемых устройствами оргтехники. Кроме того, правильно установленные фильтры могут защитить устройства оргтехники от воздействия внешних помех. Важно иметь в виду, что для эффективной работы помехоподавляющих фильтров необходимо обеспечить надежное заземление.
* Активные методы защиты сети переменного тока (220 В) включают в себя использование специальных генераторов шумовых сигналов, которые превосходят по уровню сигналы, генерируемые устройствами съема информации или информативными сигналами.

1. Блокираторы беспроводной и сотовой связи:

Блокираторы беспроводной связи разработаны с целью прекращения работы устройств, которые могут получать информацию несанкционированно. Они работают как создатели шумовых помех в соответствующих частотных диапазонах. Это позволяет регулировать мощность помехового сигнала в каждом диапазоне, обеспечивая блокирование беспроводных стандартов связи только внутри защищаемого помещения.

1. Пространственное зашумление:

При использовании различных устройств, таких как компьютеры, возникают побочные электромагнитные излучения и наводки (ПЭМИН), которые могут содержать конфиденциальную информацию. Эти сигналы могут быть перехвачены специальной аппаратурой.

Для защиты информации от утечки через каналы ПЭМИН существуют генераторы радиопомех. Они включаются в состав систем активной защиты информации (САЗ) и создают широкополосные шумовые электромагнитные помехи на границе контролируемой зоны. Это мешает распространению побочных излучений от защищаемого объекта и обеспечивает безопасность информации.

1. Защита слаботочных линий и линий связи:

Слаботочные линии и линии связи представляют потенциальную угрозу, связанную с возможностью утечки акустической информации через них. На таких линиях может возникнуть риск несанкционированного прослушивания и дешифровки переговоров, что может повлечь за собой серьезные последствия в сфере конфиденциальности и безопасности. Для предотвращения таких ситуаций и обеспечения защиты информации используются специальные устройства и стратегии, которые направлены на противодействие прослушиванию и расшифровке акустических данных, передаваемых по этим линиям.

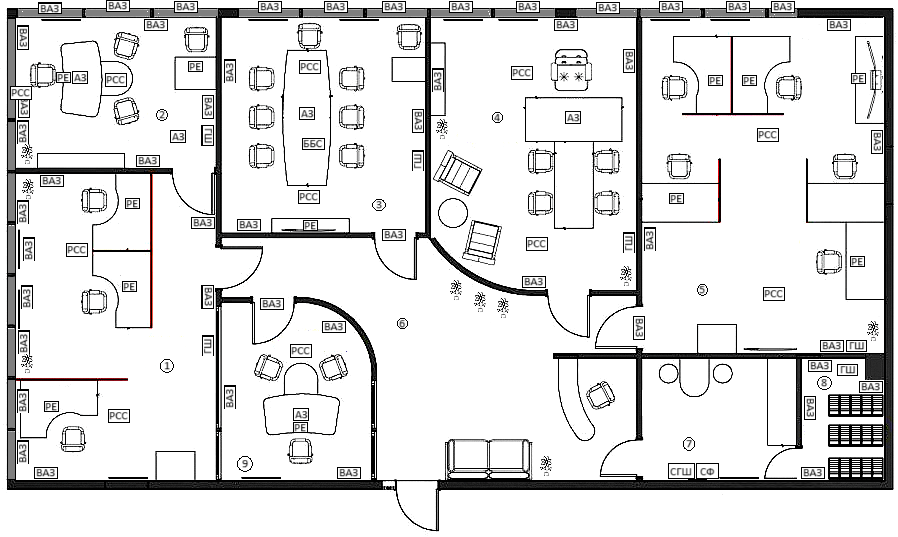
Далее я проанализировал рынок существующих решений (таблица 1) исходя из наших требований к безопасности.

Таблица 1 – Анализ рынка

|  |  |  |  |
| --- | --- | --- | --- |
| Категория | Наименование устройства | Краткое описание | Цена |
| Блокираторы беспроводной и сотовой связи | ЛГШ-702 | Плюсы: Эффективная блокировка Bluetooth и WiFi, возможность блокировки прослушивания и передачи данных, компактные размеры и небольшая масса.  Минусы: Ограниченный диапазон рабочих температур, ограниченная максимальная мощность излучения, ограниченная потребляемая мощность, отсутствие регулировки диапазона частот. | 61100 руб. |
| ЛГШ-703 | Плюсы: Эффективная блокировка сотовой связи IMT-2000/UMTS, возможность блокировки прослушивания на основе сотовых телефонов, эффективный радиус подавления, компактные размеры и небольшая масса.  Минусы: Ограниченный диапазон рабочих температур, ограниченная максимальная мощность излучения, ограниченная потребляемая мощность, ограниченный радиус действия. | 97500 руб. |
| ЛГШ-701 | Плюсы: Эффективная блокировка сотовой связи разных стандартов, работа в двух модификациях для разных диапазонов сотовой связи, регулировка мощности излучения по каждому выходу и формирование зоны подавления, высокая максимальная мощность излучения, эффективный радиус подавления, возможность использования внешних антенных устройств.  Минусы: Высокая потребляемая мощность, требующая дополнительного электропитания, ограниченный диапазон рабочих температур, большие габариты и высокая масса. | 97500 руб. |
| Акустическое зашумление | ШОРОХ 5Л | Плюсы: сертификация ФСТЭК, широкие настройки, генерация "белого шума".  Минусы: нет защиты от оптико-электронных средств, потребляет до 130 ВА. | 21500 руб. |
| ЛГШ-304 | Плюсы: соответствие требованиям ФСТЭК, визуальная индикация, счетчик времени наработки.  Минусы: ограниченные частоты, потребление не менее 10 ВА, ограниченное время работы, компактные размеры и масса. | 25220 руб. |
| Виброакустическое зашумление: | ЛГШ-404 | Плюсы: Акустическая и вибрационная защита, соответствие требованиям ФСТЭК, возможность установки в выделенных помещениях, генератор шума.  Минусы: Ограниченный диапазон частот, высокое потребление мощности, большие размеры генераторного блока. | 35100 руб. |
| ЛГШ-402 | Плюсы: Акустическая и вибрационная защита, двухканальный генератор шума, соответствие требованиям по защите акустической речевой информации, компактные габариты, низкая масса.  Минусы: Ограниченный диапазон рабочих частот, высокое потребление мощности от сети. | 18200 руб. |
| Защита сети 220/380В: | ЛФС-40-1Ф | Плюсы: Защита от электромагнитных наводок, компактные габариты.  Минусы: Ограниченный диапазон температур. | 70200 руб. |
| ЛФС-10-1Ф | Плюсы: Защита от электромагнитных наводок, компактные габариты.  Минусы: Ограниченный диапазон температур. | 47060 руб. |
| ЛФС-200-3Ф | Плюсы: Защита от электромагнитных наводок, подходит для вводно-распределительных устройств.  Минусы: Большие габариты, высокая масса, ограниченный диапазон температур. | 377000 руб. |
| ЛГШ-221 | Плюсы: индикация состояния, подходит для выделенных помещений.  Минусы: Ограниченный диапазон регулировки, высокое энергопотребление, ограниченный диапазон температур. | 36400 руб. |
| Пространственное зашумление | ЛГШ-501 | Плюсы: цена, визуальная индикация состояния, подходит для выделенных помещений.  Минусы: Ограниченный диапазон регулировки уровня шума, высокое энергопотребление, ограниченный диапазон рабочих температур. | 29900 руб. |
| ЛГШ-516СТАФ | Плюсы: соответствие требованиям для государственной тайны, регулировка уровня шума, визуальная индикация, подходит для выделенных помещений.  Минусы: Ограниченный диапазон рабочих частот, высокое энергопотребление, ограниченный диапазон рабочих температур. | 51000 руб. |
| ЛГШ-503 | Плюсы: соответствие требованиям для государственной тайны, регулировка уровня шума, визуальная индикация, подходит для выделенных помещений, возможность дистанционного управления, сертификат безопасности информации.  Минусы: Ограниченный диапазон рабочих частот, высокое энергопотребление, ограниченный диапазон рабочих температур, высокая стоимость оборудования. | 44200 руб. |
| ЛГШ-513 | Плюсы: соответствие требованиям, индикация, учет времени, защита управления, дистанционное управление, сертификат.  Минусы: Ограниченные частоты, ограниченная температура. | 39000 руб. |
| Защита слаботочных линий и линий связи | Гранит-8 | Плюсы: Гибкая настройка, Разные способы управления, Управление оповещателями, Тактики работы шлейфов, Парольная защита, Встроенный источник питания.  Минусы: Ограниченная ёмкость, Высокое потребление, Ограниченное количество событий, Ограниченное количество ключей, Ограниченные частоты. | 8070 руб. |
| ЛУР-2 | Размыкатель слаботочных линий питания, входит в состав (утверждено ФСТЭК России) системы постановки виброакустических и акустических помех «ЛГШ-404». | 5590 руб. |
| ЛУР-4 | Размыкатель слаботочных линий Телефон, входит в состав (утверждено ФСТЭК России) системы постановки виброакустических и акустических помех «ЛГШ-404». | 5590 руб. |
| ЛУР-8 | Размыкатель слаботочных Ethernet, входит в состав (утверждено ФСТЭК России) системы постановки виброакустических и акустических помех «ЛГШ-404». | 5590 руб. |

# 6. Итоговый план предприятия

В данном разделе я спроектировал полную инженерно-техническую систему защиты информации на предприятии «Сентри». Итоговый план предприятия с внедренной системой защиты представлен на Рисунке 3.



1. Внедренная инженерно-техническая система защиты информации на предприятии

Список условных обозначений:

АЗ – Система акустического зашумления;

ВАЗ – Система виброакустического зашумления;

ГШ – Генератор шума побочных электромагнитных излучений и наводок;

ББС – Блокиратор беспроводной связи;

РСС – Размыкатель слаботочных сетей;

СГШ – Сетевой генератор шума;

СФ – Сетевой фильтр для подавления помех;

РE – Размыкатель Ethernet;

# 7. Заключение

В результате выполнения курсовой работы я разработал инженерно-техническую систему защиты информации для предприятия "Сентри", которое занимается производством зашифрованных коммуникационных систем для государственных структур и спецслужб. Эта система предназначена для обеспечения безопасного обмена информацией внутри страны и между союзными государствами. В рамках выполнения задач курсовой работы я провел анализ основных характеристик и требований предприятия "Сентри". Этот анализ включал в себя выделение ключевых параметров и особенностей организации, а также оценку текущего рынка решений в данной области. В результате успешной реализации работы я разработал итоговый план предприятия, а также выполнено проектирование инженерно-технической системы защиты информации, которая удовлетворяет потребностям и особенностям деятельности предприятия "Сентри".

Таким образом, цель работы была успешно достигнута, и все поставленные задачи были выполнены.

# 8. Список использованных источников

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 с. (дата обращения: 15.12.2022).
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: https://moluch.ru/archive/107/25842/ (дата обращения: 15.12.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз. (дата обращения: 15.12.2022).
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: https://intuit.ru/studies/courses/3649/891/info (дата обращения: 15.12.2022)