**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  
системы защиты информации на предприятии»

**Выполнил:**

Алексеенко Арина Вячеславовна, студент группы N34511

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

(подпись)

**Проверил:**

Попов Илья Юрьевич, 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** | Алексеенко А.В. | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности информационных технологий | | | | | |
| **Группа** | N34511 | | |  |  |  |  |
| **Направление (специальность)** | | | | | | Информационная безопасность | |
| **Руководитель** | | Попов И.Ю., 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. Вариант 106 | | | |
| **Задание** | Проанализировать возможные каналы утечки информации в помещении, разработать | | | | | | |
| меры пассивной и активной защиты информации, рассчитать их стоимость. | | | | | | | |
|  | | | | | | | |
| **Краткие методические указания** | | | | | | | |
|  | | | | | | | |
| **Содержание пояснительной записки** | | | | | | |  |
| Курсовая работа содержит введение, теоретическую часть, анализ защищаемых помещений, выбор средств защиты информации, расчет стоимости мер защиты, заключение, список использованных источников. | | | | | | | |
| **Рекомендуемая литература** | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| Руководитель | |  | | | | | |
| Студент |  |  |  |  |  |  | (Подпись, дата) |
|  |  |  |  |  |  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

| **Студент** | Алексеенко А.В. | | | | |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности информационных технологий | | | |
| **Группа** | N34511 | | |  |  |
| **Направление (специальность)** | | | | | Информационная безопасность |
| **Руководитель** | | Попов И.Ю., 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. Вариант 106 | |

| **№**  **п/п** | **Наименование этапа** | **Дата завершения** | | **Оценка и подпись**  **руководителя** |
| --- | --- | --- | --- | --- |
| **Планируемая** | **Фактическая** |
| 1 | Заполнение задания на курсовую работу | 27.10.2023 | 27.10.2023 |  |
| 2 | Анализ материалов | 24.11.2023 | 24.11.2023 |  |
| 3 | Написание курсовой работы | 17.12.2023 | 17.12.2023 |  |
| 4 | Защита курсовой работы | 19.12.2023 | 19.12.2023 |  |

****

| Руководитель | |  |
| --- | --- | --- |
|  |  | (Подпись, дата) |
| Студент | |  |
|  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

| **Студент** | Алексеенко А.В. | | | | |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности информационных технологий | | | |
| **Группа** | N34511 | | |  |  |
| **Направление (специальность)** | | | | | Информационная безопасность |
| **Руководитель** | | Попов И.Ю., 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. Вариант 106 | |

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. **Цель и задачи работы**

Предложены студентом Сформулированы при участии студента

Определены руководителем









1. **Характер работы**

Расчет

Моделирование

Конструирование Другое: Отчет

1. **Содержание работы**

Курсовая работы включает разделы: введение, организационная структура предприятия, обоснование защиты информации, план помещения, анализ рынка, расчет стоимости мер защиты, заключение, список использованных источников. 

1. **Выводы**

В результате выполнения работы был проведен анализ каналов утечки информации в помещениях предприятия,

разработаны меры пассивной и активной защиты информации, рассчитана стоимость предложенных мер.





| Руководитель | |  |
| --- | --- | --- |
|  |  | (Подпись, дата) |
| Студент | |  |
|  |  | (Подпись, дата) |

«17» декабря 2023 г

**Содержание**

[Введение](#_2et92p0) 6

1 Анализ предприятия 7

1.1 Организационная структура предприятия 8

1.2 Обоснование секретности 8

1.3 Схема перемещения информационных потоков 14

1.4 Перечень руководящих документов 15

2 План помещения и планирование средств защиты 19

2.1 Описание помещения 19

2.2 Анализ технических каналов утечки информации 20

2.3 Выбор средств защиты 24

3 Анализ рынка технический средств защиты информации 27

3.1 Виброакустический канал утечки информации 28

3.2 Визуально-оптический канал утечки информации 29

3.3 Электромагнитный канал утечки информации 27

3.3 ПЭМИН 28

4 Внесение технических мер защиты на план здания 31

4.1 Описание расстановки технических средств защиты информации 31

4.2 План помещения с техническими средствами защиты информации 33

Заключение 34

Список используемых источников 35

# 

# **Введение**

Повсеместно на малых и крупных предприятиях происходят случаи кражи информации, которые приводят к негативным последствиям для ее владельцев. В настоящее время информацию, которая передается по различным каналам связи, требуется защищать, так как в случае слабой защиты этих каналов информация может стать доступной для посторонних лиц.

Для устранения утечек информации используются различные технические средства. Каналы, по которым информация распространяется за пределы контролируемой зоны,называются каналами утечки информации.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов, в третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий, и пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

Цель курсовой работы: разработать комплекс инженерно-технической системы защиты информации, составляющей государственную тайну с уровнем «секретно».

Задачи:

* произвести анализ технических каналов утечки информации;
* составить перечень управляющих документов;
* произвести анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;
* проанализировать рынок технических средств защиты информации;
* разработать схемы расстановки выбранных технических средств в защищаемом помещении.

# **АНАЛИЗ ПРЕДПРИЯТИЯ**

## **Организационная структура предприятия**

Полное наименование организации: АО «ДенегДай».

Область деятельности: кредитование, расчетно-кассовое обслуживание, обслуживание юридических и физических лиц, операции на валютном рынке, рынке межбанковских кредитов, операции с ценными бумагами.

Защищаемый объект состоит из семи помещений и представляет собой офис предприятия с кабинетом директора, переговорной,рабочим кабинетом, местом для отдыха, архивом, уборной и прихожей.

Режим работы:

Понедельник-пятница, 9:00 — 18:00.

Обед 13:00 — 14:00.

Часы приема граждан: вт 15:00 — 17:00, чт 10:00 — 12:00.

Информация ограниченного доступа организации:

− коммерческая тайна;

− персональные данные;

− служебная информация;

− банковская тайна;

− государственная тайна.

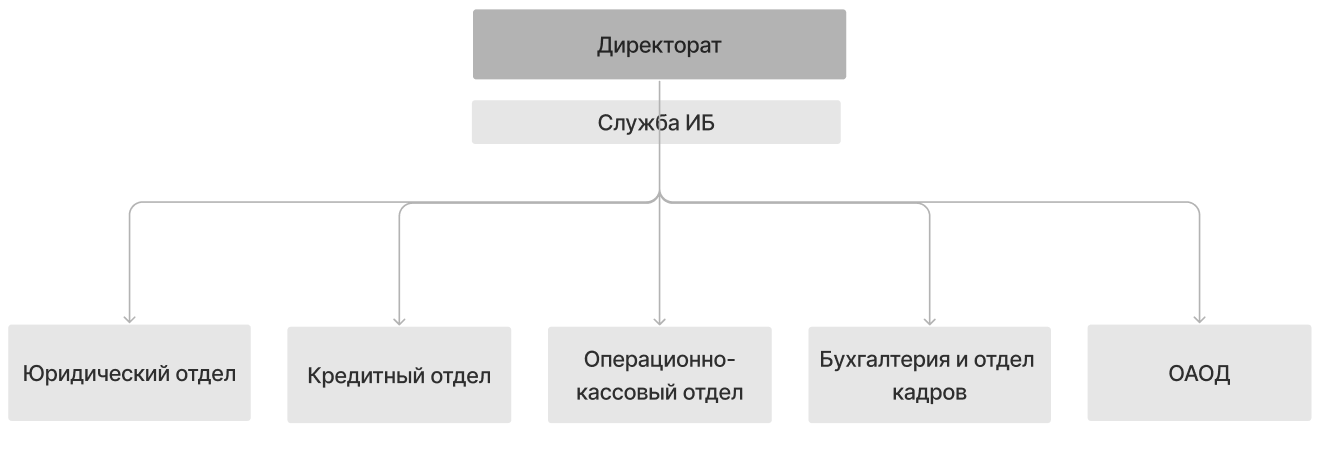


Рисунок 1 – Организационная структура предприятия

## **Обоснование секретности**

Согласно Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.:

«2.17. При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

- обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи».

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».

| 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 |
| 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 |

По постановлению Правительства РФ от 4 сентября 1995 г. N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" к секретным сведениям следует относить все сведения, отличные от сведений:

1. особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

2. совершенно секретных: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

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-розыскной области деятельности.

Соответственно класс защищенности у рассматриваемой организации 1В, так как в ней обрабатывается секретная информация и предприятие является многопользовательской АС, где не все пользователи имеют права доступа ко всей информации.

**Обоснование КИИ:**

Предприятие «ДенегДай» предназначено для выполнения функций кредитования, расчетно-кассового обслуживания, обслуживания юридических и физических лиц, операций на валютном рынке, рынке межбанковских кредитов, операций с ценными бумагами.

В состав ЛВС административного корпуса Предприятия «ДенегДай» входят

следующие системы:

− информационная система (ИС);

− автоматизированная

− система управления (АСУ) технологическим процессом;

− АСУ хозяйственной деятельностью предприятия.

АСУ ТП выполняет информационные, управляющие, контролирующие и регулирующие функции, обеспечивая контроль состояния технологического оборудования Предприятия и его защиту при возникновении нештатных ситуаций. АСУ ТП хозяйственной деятельностью выполняет информационные и управляющие функции, обеспечивая контроль информационных процессов хозяйственного блока предприятия (вписать своё).

В соответствии с абзацем третьим подпункта 4.1.1 пункта 4.1 Положения Банка России № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» *операции кредитной организации, указанные в пунктах 1 — 4 и 9 части первой статьи 5 Федерального закона № 395-1, в том числе привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок), и ведение бухгалтерского учета* следует относить к **критически важным процессам**. Кредитная организация вправе самостоятельно, исходя из характера и масштаба деятельности, определить уровень критичности процессов кредитования юридических и физических лиц. Объекту КИИ Предприятия по совокупности значений показателей в соответствии с документом «Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (утв. Постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 127) присвоена III категория значимости.

Согласно п.10 Перечня:

*Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и(или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)* – более 3, но менее или равно 70 (III категория).

Объект КИИ включает в свой состав:

− средства вычислительной техники (СВТ);

− активное сетевое оборудование (АСО);

− каналы передачи данных;

− программное обеспечение (ПО).

Оборудование ИС организации включает в себя: СВТ (34 автоматизированных рабочих мест (АРМ), 5 серверов). Перечень СВТ организации представлен в таблице 3.

Таблица 1 – Перечень СВТ организации.

| Наименование СВТ | Аппаратная платформа | Версия операционной системы (ОС) | Средство защиты информации (СрЗИ) |
| --- | --- | --- | --- |
| АРМ 1-34 | Lenovo IdeaPad I5348 | Windows 10 64-Bit | Microsoft Defender |
| Сервер 1-5 | Intel SC5300BD Microsoft | Windows Server 2019 | Microsoft Defender |

− АСО:  
 1. коммутатор Cisco SG500X-48P (7 шт.);  
 2. маршрутизатор Cisco RV340W (1 шт.).

− каналы передачи данных;

− ПО:  
 1. Windows 10 64-Bit;  
 2. ОС Windows Server 2019;  
 3. 1С Бухгалтерия;  
 4. Credit Factory;  
 5. MyCase;  
 6. Банк-Аналитика.

Сети связи расположены в пределах контролируемой зоны. Используются линии связи на основе кабелей типа «витая пара», волоконно-оптические и физические линии связи. Состав ИС организации приведен на рисунке 2, разработанном по результатам составления исходных данных для проектирования.

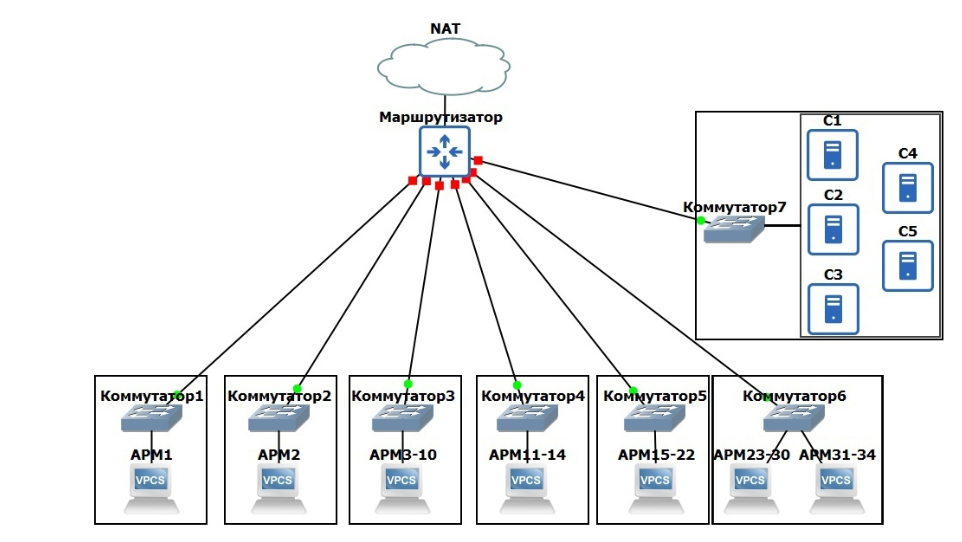


Рисунок 2 – Состав ИС

На рисунке 3 используются следующие обозначения:

− АРМ1 – управление;

− АРМ2 – пост охраны;

− АРМ3-10 – операционно-кассовый отдел;

− АРМ11-14 – бухгалтерия;

− АРМ15-22 – ОАОД;

− АРМ23-30 – кредитный отдел АРМ31-34 – юрист;

− С1 – сервер поста охраны;

− С2 – сервер операционно- кассового отдела;

− С3 – сервер ОАОД;

− С4 – сервер бухгалтерии;

− С5 – сервер кредитного отдела и юриста.

**Сведения об информационных потоках**

Департамент организации:

− операционно-кассовый отдел (10 человек);

− кредитный отдел (16 человек);

− юридический отдел (4 человека);

− бухгалтерия и отдел кадров (5 человек и 4 человека соответственно);

− отдел автоматической обработки данных (10 человек);

− правление (1 человек).

* 1. **Схема перемещения информационных потоков**

На рисунке 3 представлена схема перемещения информационных потоков, связанных с организацией. Красным помечена закрытая внутренняя информация, зелёным – открытая внутренняя, светло-зеленым – открытая внешняя:

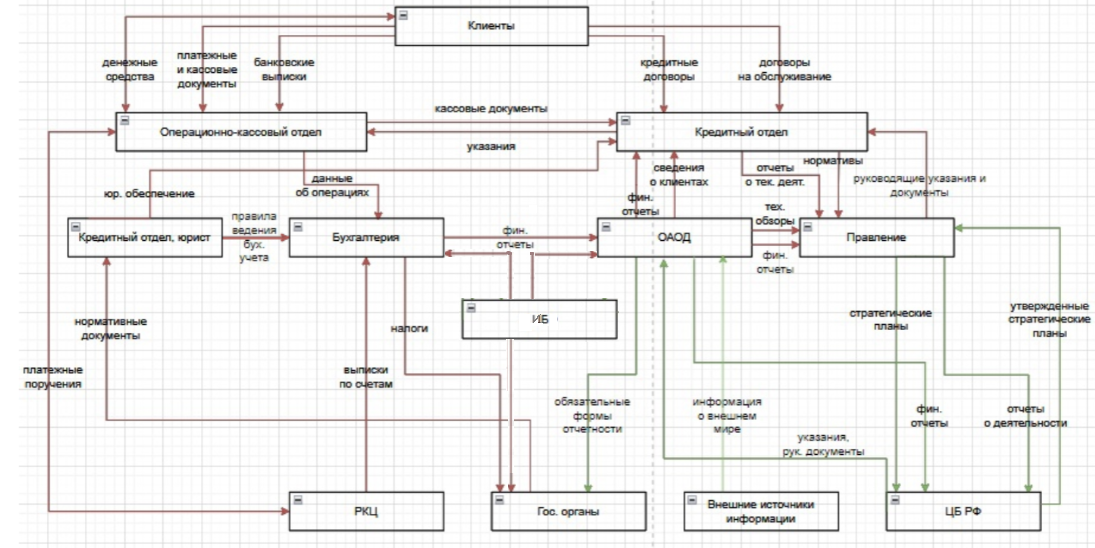


Рисунок 3 – Схема перемещения информационных потоков между организационными структурами

На рисунке 4 представлен план помещения офиса банка.

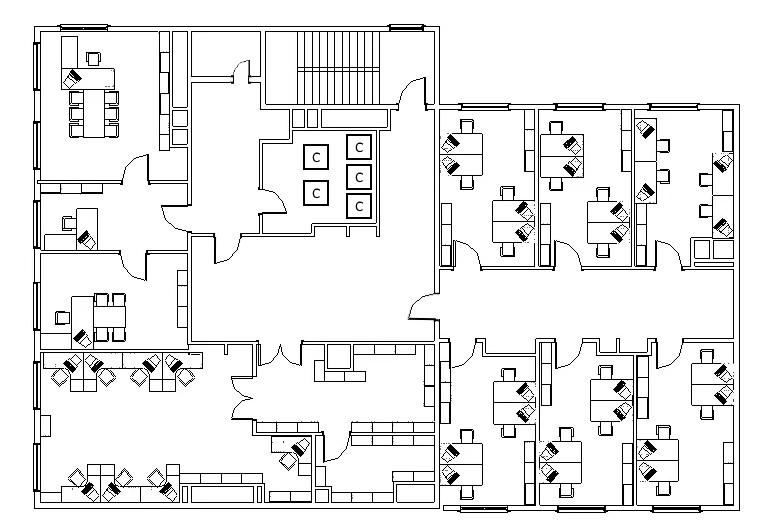


Рисунок 4 – Схема помещения

* 1. **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. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.
* Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

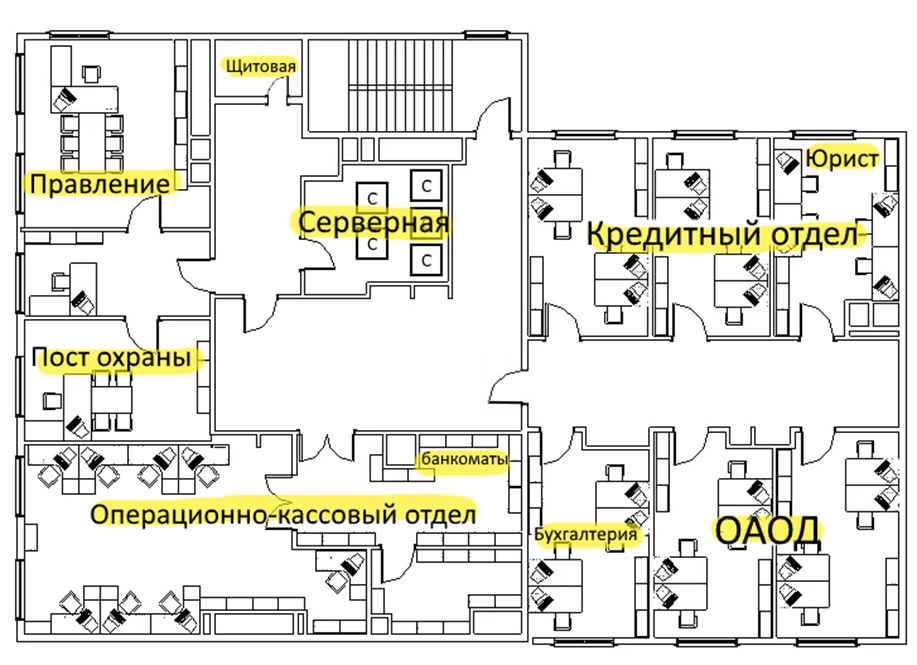
Также, необходимо обратить внимания на законы Российской Федерации:

* «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.

# **План помещения и планирование средств защиты**

**2.1 Описание помещения**

Перед тем, как перейти к разработке комплекса инженерно-технической защиты информации, необходимо описать выбранные помещения. На рисунке 5 представлен план всех помещений.

  
Рисунок 5 – План помещения до внедрения средств защиты

Для работы с клиентами предназначены два помещения (операционно-кассовый отдел и кредитный отдел), там находятся столы для приема стулья вокруг них, в сумме 5 окон. Также в операционно-кассовом отделе находятся банкоматы – важный объект с точки зрения защиты.

В кабинете директора имеется 7 мест (2 стола и ПК), 3 окна.

Пост охраны оборудован двумя столами и стульями, ПК и другим оборудованием. Имеется 1 окно.

Серверная оборудована пятью серверами.

Бухгалтерия оборудована 4 рабочими местами (стол, стул, ПК).

Помещение расположено на втором этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. Часть внутренних перегородок железобетонные, толщиной не менее 5 см, другая часть сделана из звукоизоляционного гипсокартона.

**2.2 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 6 приведена структура технического канала утечки информации.

 Рисунок 6 – 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:

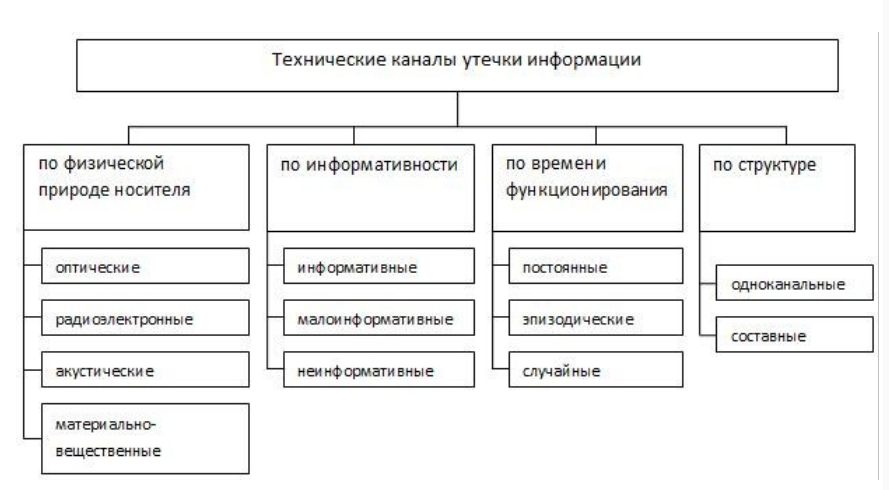
− выбор носителя с нужной получателю информацией;

− 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 7.

 Рисунок 7 – 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 приёмной 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.

**2.3 Выбор средств защиты**

Если говорить о возможных утечках информации, то в помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 1.

Таблица 1 – Активная и пассивная защита информации

| Каналы | Источники | Пассивная защита | Активная защита |
| --- | --- | --- | --- |
| акустический / акустоэлектрический | окна, двери, проводка | звукоизоляция переговорной, фильтры для сетей электро-  питания | устройства акустического зашумления |
| вибрационный / виброакустический | все твердые поверхности помещения,  батареи | изолирующие звук и  вибрацию  обшивки стен | устройства  вибрационного зашумления |
| электромагнитный / электрический | розетки, АРМы,  бытовая  техника | фильтры для сетей электропитания | устройства электромагнитного  зашумления |
| оптический | окна, двери | жалюзи /  шторы на окнах, тонирующие пленки на окна, доводчики на дверях | бликующие устройства |

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «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 см. Дверь устанавливается на металлический каркас.

1. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
2. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
3. Все режимные помещения оборудуются аварийным освещением.
4. 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.
5. 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.

# **АНАЛИЗ РЫНКА ТЕХНИЧЕСКИЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «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 секретны 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 см. 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 этаже, 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.

## **Сравнение средств защиты от утечек по виброакустическим каналам утечки информации**

Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

− усиленные двери;

− тамбурное помещение перед переговорной;

− дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Ниже в таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 2 – Сравнение средств защиты от утечек по виброакустическим каналам утечки информации

| **Модель** | **VNG-006** | **БАРОН-2** | **Соната АВ-4Б** | **Шорох** |
| --- | --- | --- | --- | --- |
| Вид помехи | аналоговый “белый шум” с нормальным распределением плотности вероятности мгновенных значений | аналоговый “белый шум” нормальным распределением плотности вероятности мгновенных значений; “речевой хор”; речеподобная; комбинированная | аналоговый “белый шум” нормальным распределением плотности вероятности мгновенных значений | аналоговый “белый шум” нормальным распределением плотности вероятности мгновенных значений |
| Максимальный уровень громкости защищаемой речевой информации, дБ | 75 | 80 | 85 | 80 |
| Полоса частот сигналов защиты, кГц | 0,175 – 5,6 | 0,06 – 16 | 0,175 – 11,2 | 0,175 – 5,6 |
| Количество независимых генераторов шума | 5 | 4 | 6 | 3 |
| Мощность, Вт | 20 | 18 | 20 | 20 |
| Сертификат ФСТЭК | Нет | Есть | Есть | Есть |
| Цена | 9 800 рублей | 62 500 рублей | 44 200 рублей | 21 500 рублей |

В результате анализа был выбран комплекс **Соната АВ-4Б**. Особенности конструкции устройства позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

Мы будем ставит не комплекс, а отдельно закупать его компоненты: **Соната-СА-4Б1** генератор- акустоизлучатель, **Соната-СВ-4Б** генератор- вибровозбудитель.

* 1. **Сравнение средств защиты от утечек по визуально-оптическим каналам утечки информации**

Пассивная защита визуально-оптического канала утечки информации представляет собой тонирующие панели, шторы, жалюзи на окна.

Активная защита предполагает систему видеонаблюдения. Рассмотрим самые популярные видеокамеры.

Таблица 3 – Сравнение средств защиты от утечек по визуально-оптическим каналам утечки информации

| **Модель** | **KDM-6301I** | **KDM-6365В** | **VG-65888LR** |
| --- | --- | --- | --- |
| Область применения | Предназначена для внутренней установки в хорошо освещенном помещении. | Может входить в состав систем видеомониторинга в торговых центрах, офисных зданиях, банках и т. д. | Камера предназначена для установки на потолок в центре помещения или на пересечении коридоров. |
| Минимальная освещенность | 0,5 Lux | 0,01 Lux | - |
| Разрешение | 380 ТВЛ | 420 ТВЛ | 520 ТВЛ |
| Ночная ИК-подсветка | Нет | до 30 метров | до 15 метров |
| Цена | 1850 рублей | 2550 рублей | 8400 рублей |

Наилучшим вариантом будет камера **KDM-6365В**, имеющая высокое разрешение, отличную дальность, небольшую цену и предназначена для офисных здани.

* 1. **Сравнение средств защиты от утечек по электромагнитным каналам утечки информации**

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания порождаемые воздействием звуковой волны или работающей электрической техникой.

Таблица 4 – Сравнение средств защиты от утечек по электромагнитным каналам утечки информации

| **Модель** | **Соната-РС3** | **Сетевой генератор шума «ЛГШ-**  **221»** | **Двухканальный**  **генератор**  **зашумления**  **SEL SP-44** |
| --- | --- | --- | --- |
| Диапазон исследуемых частот, МГц | 2000 | 400 | 400 |
| Максимальный уровень измеряемых уровней сигналов, дБ | 20 | 50 | 40 |
| Устанавливаемые полосы  пропускания | от 1 Гц  до единиц МГц | от 1 Гц  до единиц МГц | от 1 Гц  до единиц МГц |
| Устойчивость к импульсным помехам | средняя | средняя | высокая |
| Цена | 32 400 рублей | 36 400 рублей | 24 000 рублей |

В сравнении показателей и соотношении цена-качество выбор падает на Двухканальный генератор зашумления **Соната-РС3**.

* 1. **Сравнение средств защиты от утечек по ПЭМИН**

| **Модель** | **ПОКРОВ** | **ПУЛЬСАР** | **Соната Р3.1** |
| --- | --- | --- | --- |
| Возможности | Предназначен для защиты информации от утечки по техническим каналам за счет ПЭМИН путем излучения в окружающее пространство электромагнитного поля шумового сигнала и наводок на линии электропитания и заземления. | Тип "А" предназначен для нейтрализации потенциальных утечек информации через побочные электромагнитные излучения, а тип "Б" обеспечивает активную защиту от утечек через информативный сигнал на проводники. | Возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01…200 МГц за счет применения опционально поставляемой дополнительной антенны ВЕЕР. |
| Полоса частот сигналов защиты, кГц | 15 – 5600 | 10 – 6000 | 17 – 8000 |
| Устойчивость к помехам | средняя | средняя | высокая |
| Сертификат ФСТЭК | Есть | Есть | Есть |
| Цена | 32 800 рублей | 24 525 рублей | 33 120 рублей |

По всем параметрам выбор падает на **Сонату Р3.1**, как и в остальных каналах утечек.

# **ВНЕСЕНИЕ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ НА ПЛАН ЗДАНИЯ**

**4.1 Описание расстановки технических средств защиты информации**

Согласно информации, приведенной в предыдущих пунктах, выбранные средства защиты информации включают в себя:

− усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 3 шт., в переговорную, архив и кабинет директора:

− генератор шума СОНАТА-РС3;

− устройство активной защиты от ПЭМИН СОНАТА-Р3;

− 8 комплектов жалюзи на 8 окон;

− доводчики на 7 дверей.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. Согласно руководству по эксплуатации «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

− 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;

− один на окно (при установке на оконный переплет);

− 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.

Ориентировочное количество пьезоизлучателей может быть определено из расчета: один ПИ-45 на каждое стекло.

Необходимое количество аудио излучателей можно предварительно оценить из следующих норм:

− один на каждый вентиляционный канал или дверной тамбур;

− один на каждые 8...12 м3 надпотолочного пространства или др. пустот.

Основным правилом, которым следует руководствоваться при выборе мест установки излучателей в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации при обеспечении приемлемого уровня мешающего акустического шума в защищаемом помещении. Контроль вибрационного и акустического зашумления помещений рекомендуется производить в соответствии с методиками и рекомендациями ФСТЭК (Гостехкомиссии) РФ.

В таблице 5 приведена смета затрат на выбранные средства защиты информации.

Таблица 5 – Смета на выбранные средства защиты информации

| Средство защиты | Цена, руб. | Количество, шт. | Стоимость, руб. |
| --- | --- | --- | --- |
| «Соната-СА-4Б1» генератор- акустоизлучатель | 7 440 | 18 | 133 920 |
| «Соната-СВ-4Б» генератор- вибровозбудитель | 7 440 | 64 | 476 160 |
| Камера видеонаблюдения KDM-6365В | 2 550 | 17 | 43 350 |
| «Соната-РС3» генератор зашумления по по проводам электросети | 32 400 | 2 | 64 800 |
| Жалюзи | 1 300 | 14 | 18 200 |
| Дверь звукоизолирующая | 8 800 | 18 | 158 400 |
| Итого: | | | 894 830 |

**4.2 План помещения с техническими средствами защиты информации**

Жалюзи установлены на каждом окне. Элементы комплексной системы Соната «АВ» модель 4Б расположены так же, как и на рисунке 7. «Соната-PC3» подключена к системе электроснабжения согласно рекомендациям производителя.

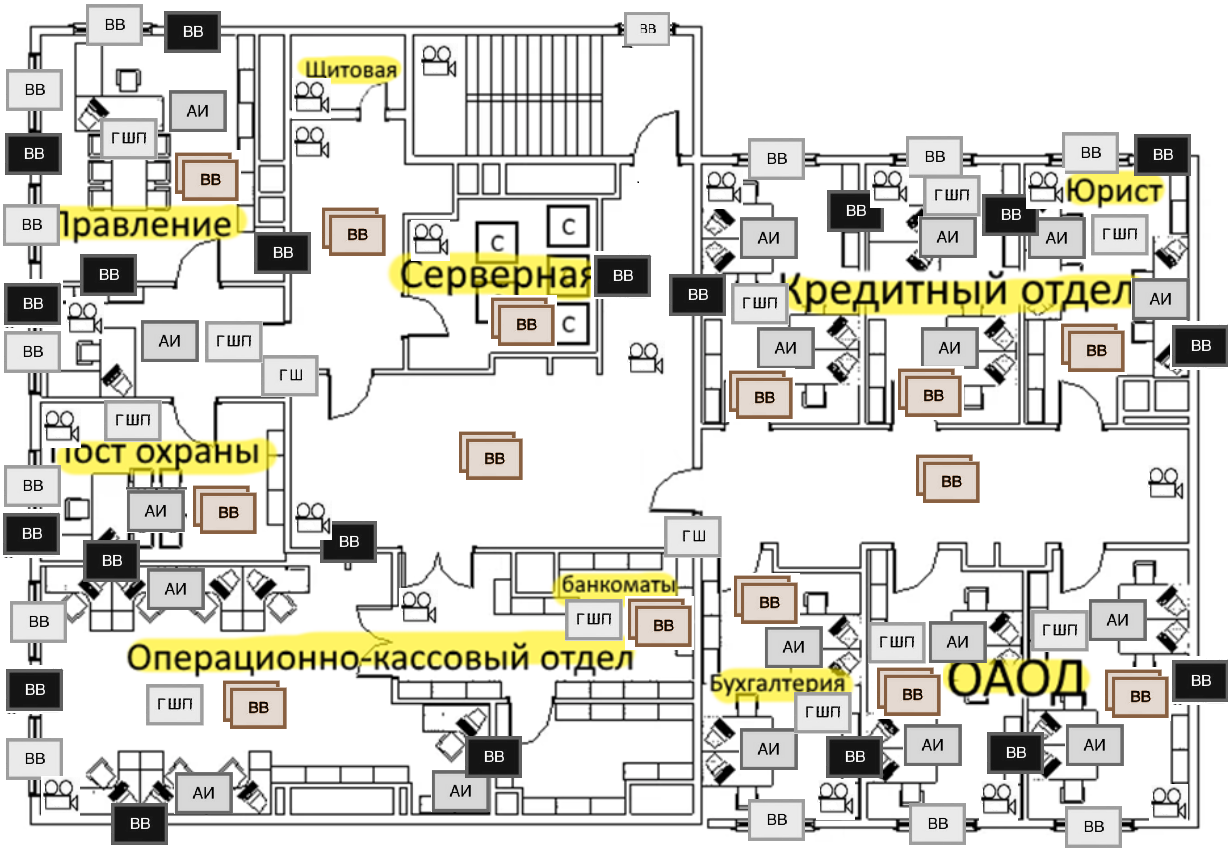


Рисунок 7 – План помещения после внедрения средств защиты

Таблица 5 – Условные обозначения средств защиты на плане помещения

| Символ | Значения |
| --- | --- |
|  | «Соната-СА-4Б» генератор-акустоизлучатель |
|  | «Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна, батареи) |
|  | «Соната-СВ-4Б» генератор-вибровозбудитель (стены) |
|  | «Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок) |
|  | «Соната-РС3» генератор зашумления по по проводам электросети |
|  | «Соната-РС3.1» генератор шума и ПЭМИН |
|  | Дверь звукоизолирующая |
|  | Камера видеонаблюдения KDM-6365В |

**Заключение**

В результате работы была спроектирована инженерно-технической

системы защиты информации на предприятии АО «ДенегДай». Организация была проанализирована на предмет структуры и информации, находящейся в обороте. Исходя из этого был проанализирован рынок технических средств защиты информации по тем каналам утечки информации, от которых они защищают:

− виброакустические каналы утечки информации;

− визуально-оптические каналы утечки информации;

− электромагнитные каналы утечки информации;

Далее активные средства защиты были спроектированы на плане здания.

**Список используемых источников**

1. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие. Лицензия ИД № 00408 от 05.11.99