

**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:

***«Применение систем контроля доступа для защиты информации на
предприятии»***

Выполнил:

Студент группы N34491

Пермин И. С.

Проверил преподаватель:

Попов И. Ю.

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Пермин И.С.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Повышение защищенности рассматриваемого помещения, принадлежащее организации

Задание Проанализировать защищаемое помещение;
 – Оценить каналы утечки информации;
 – Проанализировать рынок;
 – Выбрать меры пассивной и активной защиты информации;
 – Представить результат работы в виде схемы с установленными средствами защиты

Краткие методические указания

Составить отчёт по выполненной курсовой работе

Содержание пояснительной записки

Рекомендуемая литература

Руководитель _____

(Подпись, дата)

Студент _____



19 декабря 2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Пермин И.С.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации


Наименование темы Повышение защищенности рассматриваемого помещения, принадлежащее организации

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение титульных листов и поиск источников	01.11.2023	01.11.2023	
2	Анализ информации	02.11.2023	02.11.2023	
3	Написание курсовой работы	14.11.2023	14.11.2023	
4	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель _____

(Подпись, дата)

Студент _____


19 декабря 2023

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент Пермин И.С.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Повышение защищенности рассматриваемого помещения, принадлежащее организации

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА
(РАБОТЫ)**

**1. Цель и задачи
работы**

☒ Предложены студентом

☐ Сформулированы при участии студента

☐ Определены руководителем

**2. Характер
работы**

☒ Расчет

☐ Конструирование

☐ Моделирование

Другое: Исследовательская
работа

3. Содержание работы

В работе представлены существующие и потенциальных каналы утечки информации в защищаемых в рамках курсовой работы помещениях, схемы помещения, возможные средства обеспечения защиты от утечек, выбраны и расставлены средства защиты информации.

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель _____

(Подпись, дата)

Студент _____



19 декабря 2023

(Подпись, дата)

«19» декабря 2023 г

Содержание

ВВЕДЕНИЕ	6
2. ПОСТАНОВКА ЗАДАЧ	7
1.1. Цель курсовой работы	7
1.2. Задачи, решаемые в ходе выполнения данной работы:	7
ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ	8
2.1 Анализ технических каналов утечки информации.....	8
2.2 Перечень руководящих документов по защите информации	11
1. Законы Российской Федерации:	11
2. Указы Президента Российской Федерации:.....	11
3. Постановления Правительства Российской Федерации:	12
4. Решения Гостехкомиссии России:	13
5. Руководящие и нормативно-методические документы Гостехкомиссии России:	14
2.3 Анализ выбранного помещения	17
2.3.1 Общая информация о предприятии	17
2.3.2 Описание помещения	19
2.4 Анализ технических каналов утечки информации и выбор средств защиты	23
2.5 Анализ технических средств защиты информации	25
2.5.1 Системы защиты от акустических сигналов	25
2.5.2 Средства защиты от электромагнитных излучений и ПЭМИН	27
2.5.3 Средства защиты от ПЭМИН	30
2.5.3 Защита от утечек по оптическому каналу	31
2.6 Описание расстановки технических средств защиты информации	32
ЗАКЛЮЧЕНИЕ	34
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	35

Введение

Утечка конфиденциальной информации представляет большую угрозу для компаний и организаций, влекая серьезные негативные последствия. Причины утечек могут быть как умышленные (действия злоумышленников), так и непреднамеренные (ошибки сотрудников).

Цели злонамеренных атак включают нанесение вреда, получение прибыли или конкурентных преимуществ. Неумышленные утечки часто происходят из-за небрежности персонала

Для защиты от утечек информации нужен профессиональный подход с использованием передовых технологий. Это включает выявление и блокирование потенциальных каналов утечек, а также соответствие стандартам информационной безопасности.

Ключевыми задачами являются определение угроз и уязвимостей системы, а также возможных технических каналов утечек. При этом важно анализировать все элементы системы, от основного оборудования до вспомогательных систем электроснабжения и вентиляции.

Для эффективной защиты нужен комплексный подход, включающий человеческие, технические и организационные аспекты. Компании должны инвестировать в обучение сотрудников, мониторинг угроз и обновление систем безопасности.

2. Постановка задач

1.1. Цель курсовой работы

Повышение защищенности рассматриваемого помещения, принадлежащее организации

1.2. Задачи, решаемые в ходе выполнения данной работы:

- Проанализировать защищаемое помещение;
- Оценить каналы утечки информации;
- Проанализировать рынок;
- Выбрать меры пассивной и активной защиты информации;
- Представить результат работы в виде схемы с установленными средствами защиты

ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ

2.1 Анализ технических каналов утечки информации

Утечка информации — это неконтролируемое распространение сведений, составляющих коммерческую или государственную тайну, за пределы организации или определенного круга посвященных лиц. Такая утечка происходит по специальным каналам передачи данных и нарушает безопасность информационных систем.

Выделяют три основные группы каналов утечки:

- разглашение информации;
- несанкционированный доступ к информации;
- утечка информации по техническим каналам

В данной работе рассматриваются только технические каналы.

Технический канал утечки представляет собой путь прохождения информационного сигнала от носителя конфиденциальных данных через физическую среду распространения до технического устройства, которое осуществляет перехват и декодирование этого сигнала.

Рассмотрим более подробно элементы технического канала утечки информации.

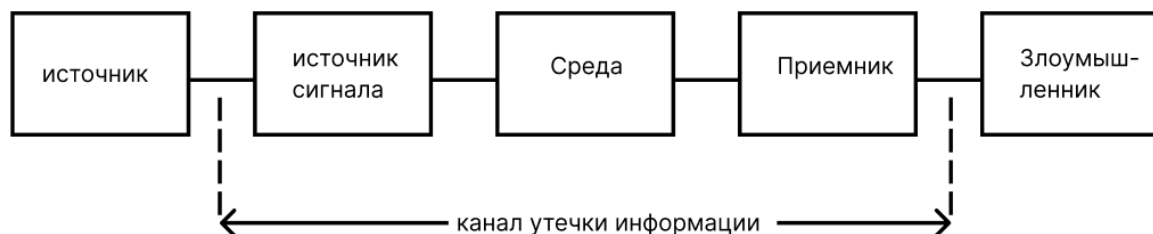


Рисунок 1 - Структура технического канала утечки информации

Технический канал утечки информации (ТКУИ) представляет собой систему, объединяющую объект технической разведки, физическую среду

передачи информации и средства, используемые для извлечения защищенных данных.

Источниками информационного сигнала могут быть различные объекты, такие как:

- предметы отражающие электромагнитные и акустические волны;
- предметы излучающие собственные электромагнитные волны;
- передатчики связи;
- закладные устройства;
- источники опасных сигналов и
- акустические источники, модулированные информацией.

Полученная информация затем преобразуется таким образом, чтобы ее можно было записать на носитель информации, соответствующий среде передачи. Среда передачи сигнала - это физическая среда, по которой информационный сигнал может распространяться и регистрироваться приемником, характеризуясь различными физическими параметрами, такими как препятствия для передачи сигнала, ослабление сигнала, частотная характеристика и помехи.

Среда может быть однородной (например, вода, воздух, металл) или неоднородной, возникающей при переходе сигнала из одной среды в другую, например, при акустоэлектрических преобразованиях.

Приемник выполняет обратные функции передатчика, включая выбор носителя с нужной информацией, усиление принятого сигнала, извлечение информации с носителя, преобразование информации в форму, доступную получателю (человеку или техническому устройству) и усиление сигналов для безошибочного восприятия.

Технические каналы утечки информации классифицируются по физической природе носителя на оптические, радиоэлектронные, акустические и материально-вещественные. Например, оптический канал использует электромагнитное поле (фотоны). Оптический диапазон

подразделяется на: дальний инфракрасный поддиапазон 100 - 10 мкм, средний и ближний инфракрасный поддиапазон 10 - 0,76 мкм, и видимый диапазон 0,76 - 0,4 мкм. Радиоэлектронный канал включает в себя диапазоны от низкочастотного 10 - 1 км до сверхвысокочастотного 3 - 30 ГГц. Носителями информации в акустическом канале являются упругие акустические волны, с диапазонами от инфразвукового 1500 - 75 м до ультразвукового $< 0,2$ м (> 16000 Гц) и до 4 МГц.

2.2 Перечень руководящих документов по защите информации

Нормативные документы по противодействию технической разведке:

1. 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.

2. Указы Президента Российской Федерации:

«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.

3. Постановления Правительства Российской Федерации:

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.

4. Решения Гостехкомиссии России:

«Основы концепции защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам» от 16 ноября 1993 г. № 6.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации» от 14 марта 1995 г. № 32.

«Типовое положение о Совете (технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам» от 14 марта 1995 г. № 32.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (учреждении, организации)» от 14 марта 1995 г. № 32.

«О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте» от 3 октября 1995 г. № 42.

«Методические рекомендации по разработке развернутых перечней сведений, подлежащих засекречиванию» от 3 февраля 1995 г. № 29.

«Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)» от 23 мая 1997 г. № 55.

«Положение о государственном лицензировании деятельности в области защиты информации (Решение Гостехкомиссии России и ФАПСИ)» от 27 апреля 1994 г. № 10 с дополнениями и изменениями, внесенными Решением Гостехкомиссии России и ФАПСИ от 24 июня 1997 г. № 60.

Положение о головной научно-исследовательской организации по проблеме защиты информации (Решение Председателя Гостехкомиссии

России) от 15 марта 1993 г.

Пособие по проектированию технических мероприятий защиты военнопromышленных объектов от ИТР (Пособие к ВСН-01-82). Утверждено НИИА и согласовано с Гостехкомиссией СССР в 1983 г., переутверждено Решением Гостехкомиссии России от 13 ноября 1990 г, № 89–3.

«О защите информации при вхождении России в международную информационную систему «Интернет» от 21 октября 1997 г. № 61.

5. Руководящие и нормативно-методические документы Гостехкомиссии России:

Руководящий документ (РД). Защита от несанкционированного доступа (НСД) к информации. Термины и определения. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по ЗИ. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии

России от 25 июля 1997 г.

РД. Защита информации Специальные защитные знаки. Классификация и общие требования. Решение Председателя Гостехкомиссии России от 25 июля 1997г.

Модель ИТР-2010. Решение Гостехкомиссии России от 16 августа 1996 г. № 49. Методики оценки возможностей ИТР (МВТР-87) (с изменениями)

Решение Гостехкомиссии СССР от 16 сентября 1987 г. №70-3, извещения № 1-88, № 2-90, № 3-91, № 4-93.

Нормативно-методические документы (НМД) по противодействию (ПД) средствам иностранной радиотехнической разведки.

Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

Нормативно-методические документы по противодействию иностранной радиоразведке.

Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

Нормативно-методические документы по противодействию средствам иностранной фоторазведки и оптикоэлектронной разведки. Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

Нормативно-методические документы по противодействию средствам иностранной гидроакустической разведки. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

Нормативно-методические документы по противодействию радиолокационным средствам иностранной воздушной и космической разведок. Решение Гостехкомиссии России от 16 ноября 1993г. № 7.

Нормативно-методические документы по противодействию радиационной разведке. Решение Гостехкомиссии России от 15 ноября 1994 г. № 25.

Нормативно-методические документы по противодействию тепловизионным

средствам иностранной инфракрасной разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной химической разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной разведки лазерных излучений. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной акустической (речевой) разведки. Решение Гостехкомиссии России. 1991 г.

Нормы эффективности защиты АСУ и ЭВТ от утечки информации за счет ПЭМИН.

Решение Председателя Гостехкомиссии СССР, 1977 г.

Нормы эффективности защиты технических средств передачи телевизионной информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13, от 30 ноября 1987г. № 11-3.

Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13.

2.3 Анализ выбранного помещения

2.3.1 Общая информация о предприятии

Наименование организации: ООО «Яблочные»

Область деятельности: Торговля оптовая бытовыми электротоварами

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа: Организации, занимающиеся оптовой торговлей бытовой техникой, ведут разнообразные информационные процессы и потоки, чтобы обеспечивать эффективное управление бизнесом и удовлетворять потребности клиентов.

Основные информационные процессы и потоки в организации:

1. Закупки и поставки:

- Организации закупают бытовую технику у производителей и поставщиков.
- Информация о доступных товарах, ценах, объемах и сроках поставки важна для принятия решений о закупках.

2. Складское управление:

- Информация о состоянии запасов на складе и о движении товаров (прием, отправка, инвентаризация) помогает оптимизировать управление запасами и предотвращать дефициты или избытки.

3. Продажи и заказы:

- Организация принимает заказы от клиентов и обрабатывает продажи оптовой бытовой техники.
- Информация о заказах, статусах и запросах клиентов управляется в системе учета заказов.

4. Логистика и доставка:

- Для оптовых продаж важно следить за логистикой и доставкой товаров клиентам.
- Информация о маршрутах, доставках, адресах клиентов и расписаниях играет роль в этом процессе.

5. Финансовое управление:

- Учет финансовых операций, включая выставление счетов, оплаты, налоги и бухгалтерские записи, является неотъемлемой частью управления организацией.

6. Управление клиентскими данными:

- Организации могут использовать CRM-системы для управления информацией о клиентах, их заказах, предпочтениях и истории взаимодействия.

7. Маркетинг и реклама:

- Информационные процессы в области маркетинга включают анализ рынка, аудитории и рекламные кампании для привлечения клиентов.

8. Аналитика и прогнозирование:

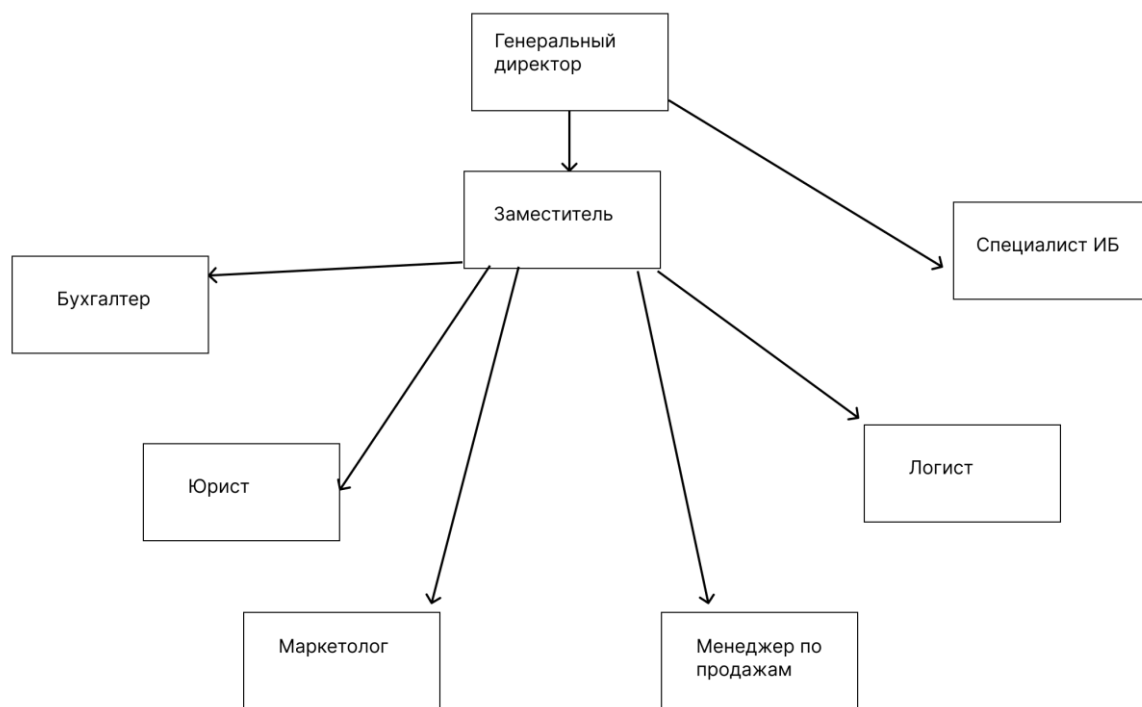
- Использование аналитических инструментов и данных помогает организации принимать стратегические решения, такие как прогнозирование спроса и оптимизация ассортимента товаров.

9. Информация ограниченного доступа:

- В определенных случаях информация о клиентах, контрактах, ценах и скидках может считаться ограниченной и требовать повышенной защиты и доступа только уполномоченных сотрудников.

10. Соблюдение норм и законов:

- Организации должны соблюдать законы и нормативы, касающиеся торговли и хранения бытовой техники, что также требует информационной поддержки.



Информация ограниченного доступа:

1. Персональные данные сотрудников
2. Персональные данные клиентов
3. Техническая информация
4. Коммерческая тайна
5. Государственная тайна

2.3.2 Описание помещения

Рассмотренный в данной курсовом проекте объект защиты представляет собой помещение, расположенное на 1 этаже малоэтажного здания. План помещения представлен на рисунке №. Помещения на плане пронумерованы в соответствии с названиями:

1. Кабинет директора
2. Офис
3. Системы резервного питания
4. Комната охраны

5.1 Рабочее место системного администратора со стеклянной

перегородкой

5.2 Серверная

6. Туалет

7. Холл

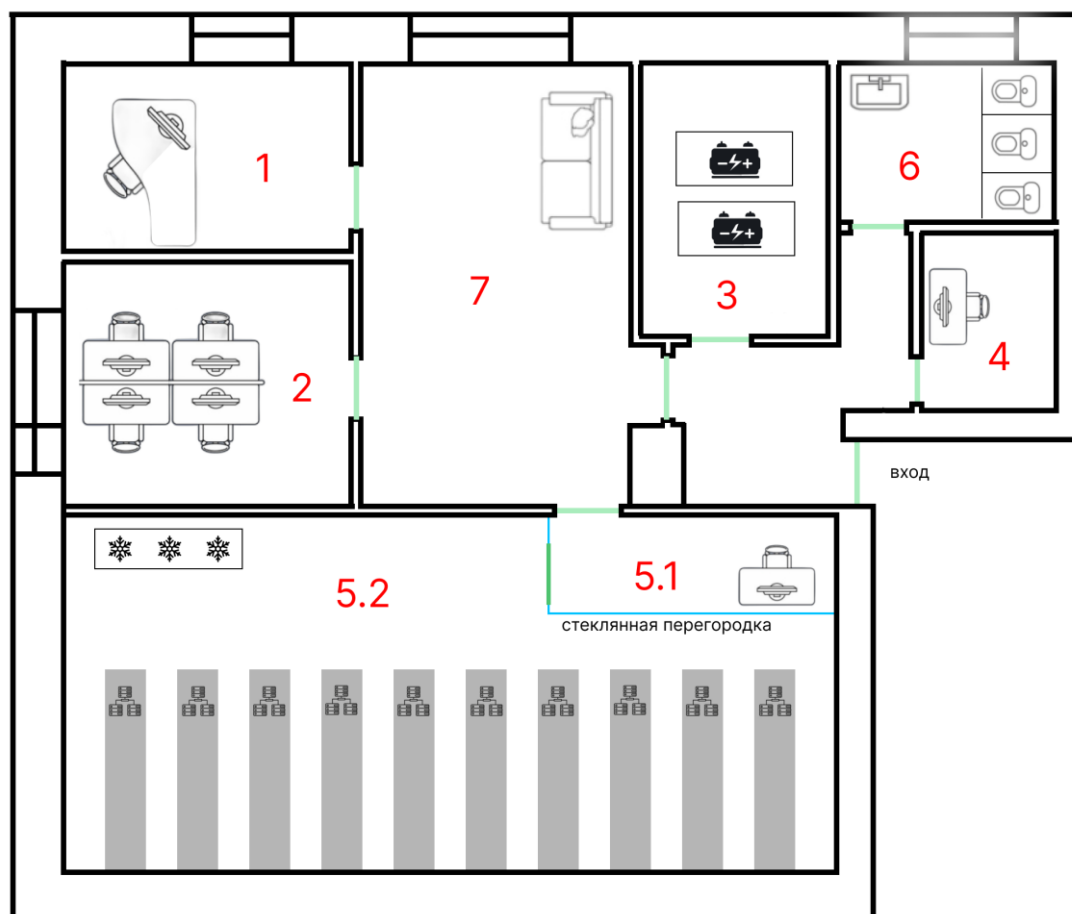
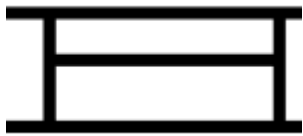


Рисунок 2 – План помещения

В таблице 1 приведено описания всех элементов, изображенных на плане помещения.

Таблица 1 - Описание элементов, изображенных на плане помещения

Обозначение	Описание
	Окно

	РМ начальника
	РМ сотрудников
	Диван
	Системы резервного питания
	Раковина
	Унитаз
	РМ системного администратора/охранника
	Холодильная машина

	Сервер
	Дверь
	Стеклянная перегородка

Помещения, требующие защиты:

Кабинете директора: 3м на 4 м – 12м²

Офис: 4м на 4м - 16м²

Системы резервного питания: 4м на 5м - 20м²

Комната охраны: 2м на 3м - 6м²

Серверная с кабинетом системного администратора: 6м на 12м - 72м²

2.4 Анализ технических каналов утечки информации и выбор средств защиты

Для ведения переговоров предназначено одно помещение - кабинет директора.

В кабинете директора: 1 окно, 1 стол, 1 стул, 1 компьютер, 3 розетки, 1 батарея центрального отопления.

В офисе 1 окно, 1 батарея центрального отопления, 4 рабочих места с АРМ, 8 розеток.

В серверной располагается 10 серверных стоек, 1 АРМ, 6 розеток.

Помещение расположено на 1 этаже одноэтажного 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. На окнах установлены решетки.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

В каждом помещении имеются розетки, а значит, актуальны каналы электрического и электромагнитного утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, вибро-акустическому, 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 активными и пассивными средствами защиты информации.

Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен

звукопоглощающими материалами или экранирования технических средств.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещению средствам защиты, приведенными в таблице 2.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Акустический акустоэлектрический	Проводка, двери, окна	Сетевые фильтры, звукоизоляция	устройства акустического зашумления
Вибрационный виброакустический	Батареи, трубы, стены, пол, окна, двери	Изолирующие звук и вибрацию материалы стен	устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах/шторы, доводчики на двери	блокирующие обзор устройства
Электромагнитный электрический	Арм, бытовые приборы, розетки	Сетевые фильтры	устройства электромагнитного зашумления

2.5 Анализ технических средств защиты информации

2.5.1 Системы защиты от акустических сигналов

Пассивная защита представляет собой:

- Усиленные двери;
- Сетевые фильтры
- Изолирующие звук и вибрацию материалы стен

В качестве пассивной защиты выбраны звукоизоляционные усиленные двери Rw Prima M900 стоимостью 40к руб.

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 1Б. Ниже в таблице 3 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналам.

Таблица 3 – Сравнительный анализ средств активной защиты для виброакустического канала

Наименование средства	Система активной акустической и вибрационной защиты акустической речевой информации Соната «АВ» модель 4Б	Система постановки виброакустических помех ЛГШ-403	Генератор маскирующего шума «Камертон-5»
Характеристики	- Сертификат ФСТЭК - Диапазон частот 175 – 11200 Гц -	- Сертификат ФСТЭК - Диапазон частот 175 – 11200 Гц -	- Сертификат ФСТЭК - Диапазон частот 90 - 11200 Гц -

	Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам.	Изделие предназначено для защиты акустической речевой информации, циркулирующей в помещениях, предназначенных для обсуждения или воспроизведения, а также проведения мероприятий с обсуждением информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки информации по виброакустическому и акустическому каналам.	Предназначен для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов
Цена (руб.)	44200	18200	46000

По результатам проведенного анализа средств защиты, в качестве системы виброакустической защиты была выбрана «ЛГШ-403».

В состав ЛГШ-403 входят:

- Генератор шума ЛГШ-403
- Вибропреобразователь для стен, полов, потолков ЛВП-2с
- Вибропреобразователь для окон ЛВП-2о

- Акустический излучатель ЛВП-2а
- Вибропреобразователь для трубопроводов ЛВП-2т
- Размыкатели ЛУР

2.5.2 Средства защиты от электромагнитных излучений и ПЭМИН

Технические устройства, не являющиеся радиопередатчиками, создают нежелательные электромагнитные излучения, называемые побочными. Они возникают из-за:

- Излучений элементов самих устройств.
- Излучений на частотах работы высокочастотных генераторов.
- Излучений усилителей низкой частоты.

Электрические каналы утечки информации появляются из-за:

- Наводок излучений технических средств на линии связи и проводники.
- Просачивания сигналов в линии электропитания и заземления.
- Использования закладных устройств.

В разных устройствах протекают переменные электрические токи, создающие электромагнитные поля, излучаемые в пространство. Их структура и параметры зависят от особенностей устройств, условий размещения и работы. Такие излучения несут потенциально опасный сигнал.

Технические средства различного назначения могут иметь в своем составе устройства, которые для выполнения своих основных функций генерируют электромагнитные колебания (эталонные и измерительные генераторы, генераторы тактовых частот)

В таблице 4 представлен сравнительный анализ

Таблица 4 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение/состав	Цена (руб.)
«Соната-РСЗ» – устройство для защиты линий электропитания и заземления от утечки информации	Диапазон частот до 2 ГГц	Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения и обеспечивают формирование несинфазных токов и синфазных и парафазных составляющих шумового напряжения во всех проводниках. Возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения; совместимость с проводными пультами ДУ линейки СОНАТА	32 400р
Генератор шума Покров, исполнение 1	Диапазон шумового сигнала -для электрической составляющей 0,01 – 6000 МГц - для магнитной составляющей 0,01 – 30 МГц - для электрических сигналов, наведённых на цепи электропитания 0,01 – 400 МГц	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. Имеется сертификат ФСТЭК России №4324 от 18.11.2020,	32 800р

		действителен до 18.11.2025	
Двухканальный генератор зашумления SEL SP-44	Спектральная плотность напряженности электрического поля шума 0,01 – 1 МГц 90дБ / 1 – 10 МГц 70 дБ / 10 – 100 МГц 50 дБ / 100 – 300 МГц 35 дБ	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Индикация нормального/ аварийного режима работы. Электропитание от сети переменного тока 220В 50 Гц. Устройство имеет высший классустойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания	24 000р
Сетевой генератор шума ЛГШ-221	Спектральная плотность напряжения шумового сигнала в диапазоне частот 10 ÷ 500 кГц, дБ(мкВ/√кГц) – 10 ÷ 50 / в диапазоне частот 0,5 ÷ 30 МГц, дБ(мкВ/√кГц) – 10 ÷ 58 / в диапазоне частот 30 ÷ 400 МГц, дБ(мкВ/√кГц) – 10 ÷ 47	Сертификат ФСТЭК России по 2 классу защиты. Может устанавливаться в ВП до 2 категории. Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Световой индикатор работы в стандартном режиме; световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы; счетчик отработанных часов; возможность интеграции в программноаппаратный комплекс ДУ и контроля «Паутина»	36 400р

Фильтр сетевой помехоподавляющий ФСПК-100	Номинальный рабочий ток не более 100 А. Режим работы устройство допускает непрерывную круглосуточную работу в течение длительного времени (не менее 1 года)	Принцип действия – подавление (фильтрация) помех в частотном диапазоне от 0,1 до 1000 МГц. Фильтр обеспечивает электромагнитную развязку в цепях электропитания электросетей объектов промышленного и непромышленного назначения, и различной вычислительной и радиоэлектронной техники. Каждый полукomплект состоит из: металлического основания; двух токонесущих латунных (медных) шин с устройствами подключения; шести цилиндрических корпусов двенадцати конденсаторов по 10 мкФ каждый	267 000р

На основании проведенного анализа средств активной защиты в электрических, акустоэлектрических и электромагнитных каналах утечки информации, принял решение использовать двухканальный генератор зашумления SEL SP-44, имеющий низкую стоимость по сравнению с конкурентами и большой диапазон частот, также имеет высший класс устойчивости к импульсным помехам.

2.5.3 Средства защиты от ПЭМИН

В дополнение для защиты от ПЭМИН буду использовать генератор шума

Покров, исполнение 1, который выполнен в виде сетевого удлинителя с 5 розетками и сертифицирован ФСТЭК

2.5.3 Защита от утечек по оптическому каналу

В качестве средства защиты информации от утечек по оптическому каналу через окна достаточно использовать любые доступные на рынке плотные офисные шторы или жалюзи. С точки зрения удобства содержания были выбраны жалюзи.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

2.6 Описание расстановки технических средств защиты информации

На основании анализа, приведенного выше были выбраны технические средства защиты:

Оптический канал:

Жалюзи

Дверной доводчик

Электромагнитный канал:

SEL SP-44 -генератор зашумления

Генератор шума Покров, исполнение 1

Виброакустический канал:

Rw Prima M900 - звукоизоляционные усиленные двери

Генератор шума ЛГШ-403

Вибропреобразователь для стен, полов, потолков ЛВП-2с

Вибропреобразователь для окон ЛВП-2о

Акустический излучатель ЛВП-2а

Вибропреобразователь для трубопроводов ЛВП-2т

Размыкатели ЛУР



- Ж Жалюзи (4 шт)
- ДД Дверной доводчик (9шт)
- SS SEL SP-44 -генератор шумления (4шт)
- П1 Генератор шума Покров, исполнение 1 (5шт)
- RPM Rw Prima M900 - звукоизоляционные усиленные двери (1шт)
- ЛГШ 403 Генератор шума ЛГШ-403 (3шт)
- ЛВП 2с Вибропреобразователь для стен, полов, потолков ЛВП-2с (11 шт)
- ЛВП 2о Вибропреобразователь для окон ЛВП-2о (4шт)
- ЛВП 2а Акустический излучатель ЛВП-2а (5шт)
- ЛВП 2г Вибропреобразователь для трубопроводов ЛВП-2г (4шт)
- ЛУР Размыкатели ЛУР (3шт)

ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта мной была разработана инженерно-техническая система защиты информации для организации ООО “Яблочные”.

Для достижения цели мною было проведено предпроектное обследование организации и выявлены основные информационные активы, внешние и внутренние, открытые и закрытые информационные потоки, а также был обследован план помещения организации и выявлены возможные каналы утечки информации.

Также мною был проведен анализ нормативной базы, с целью выявления обоснования для защиты информации и анализ рынка инженерно-технических средств, с целью выявления наилучших предложений.

Результатом обследования организации и анализа нормативной базы является план помещения предприятия с инженерно-технической системой защиты информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. – 151с. – экз.
2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436