

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

**«Проектирование инженерно-технической защиты информации на предприятии.
Вариант 105»**

Выполнил:

Алеева А.Р., студент группы N34511



(подпись)

Проверил:

Попов И.Ю., к.н.т. доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Алеева А.Р. (Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Информационная безопасность
Руководитель	Попов И.Ю., к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 105
Задание	Спроектировать инженерно-техническую систему защиты информации на предприятии.

Краткие методические указания

Содержание пояснительной записки

В курсовой работе проводится анализ организационной структуры предприятия, видов обрабатываемой там информации, составляющей государственную тайну, плана помещения, средств защиты, а также проектирование плана помещения уже с внедренной активной и пассивной защитой.

Введение

1. Общие положения
2. Каналы утечки информации
3. Исследование помещений предприятия
4. Технические средства защиты информации для рассматриваемого предприятия

Заключение

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	 Алеева Амина Рамилевна 21.12.2023 (Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Алеева А.Р.
(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

**Направление
(специальность)** 10.03.01 Информационная безопасность


Руководитель Попов И.Ю., к.т.н., доцент ФБИТ
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

**Наименование
темы** Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 105

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Составление плана курсовой работы	17.11.2023	17.11.2023	
2	Анализ материалов	24.11.2023	24.11.2023	
3	Написание курсовой работы	07.12.2023	07.12.2023	
5	Защита курсовой работы	21.12.2023	26.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент  Алеева Амина Рамилевна 21.12.2023
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Алеева А.Р. (Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Информационная безопасность
Руководитель	Попов И.Ю., к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 105

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом ☐ Сформулированы при участии студента

☒ Определены руководителем

2. Характер работы

☐ Расчет ☒ Конструирование

☐ Моделирование ☐ Другое:

3. Содержание работы

Введение

1. Общие положения
2. Каналы утечки информации
3. Исследование помещений предприятия
4. Технические средства защиты информации для рассматриваемого предприятия

Заключение

4. Выводы

В результате выполнения работы был проведен теоретический анализ технических каналов утечки информации, анализ выбранного предприятия и обрабатываемой там информации, рынка инженерно-технических средств защиты информации, а также выполнено проектирование инженерно-технической системы защиты информации.

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент



Алеева Амина Рамилевна 21.12.2023

(Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
1 ОБЩИЕ ПОЛОЖЕНИЯ.....	7
1.1 Общие сведения о защищаемой организации.....	7
1.2 Законодательство в области защиты информации.....	7
2 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ.....	9
2.1 Общие сведения о технических каналах утечки информации.....	9
2.2 Описание технических каналов утечки информации.....	12
2.2.1 Оптические каналы утечки информации.....	13
2.2.2 Радиоэлектронные каналы утечки информации.....	14
2.2.3 Акустические каналы утечки информации.....	15
2.2.4 Материально-вещественные каналы утечки информации.....	16
3 ИССЛЕДОВАНИЕ ПОМЕЩЕНИЙ ПРЕДПРИЯТИЯ.....	18
3.1 Обоснование необходимости защиты информации.....	18
3.2 План и описание помещений предприятия.....	19
3.3 Анализ возможных утечек информации.....	21
4 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ РАССМАТРИВАЕМОГО ПРЕДПРИЯТИЯ.....	23
4.1 Анализ рынка технических средств.....	23
4.1.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации.....	23
4.1.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	24
4.1.3 Устройства для перекрытия утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН).....	25
4.1.4 Устройства для перекрытия оптического канала утечки информации.....	25
4.2 Описание расстановки технических средств.....	26
4.3 План помещения с активной и пассивной защитой.....	28
ЗАКЛЮЧЕНИЕ.....	30
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	31

ВВЕДЕНИЕ

В современном мире информация играет ключевую роль в деятельности любого предприятия. От ее качества, достоверности и своевременности получения зависит эффективность работы предприятия и его конкурентоспособность на рынке. В то же время информация является объектом интереса злоумышленников, которые стремятся получить доступ к конфиденциальным данным.

Одним из основных направлений обеспечения информационной безопасности является внедрение инженерно-технической системы защиты информации. Эта система представляет собой комплекс мер, направленных на предотвращение несанкционированного доступа, утечки, искажения или уничтожения информации.

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

Для достижения цели необходимо решить следующие задачи:

- изучить теоретические и правовые основы;
- рассмотреть и описать технические каналы утечки информации;
- исследовать помещения рассматриваемого предприятия на предмет возможных утечек информации;
- провести анализ рынка и выбрать средства защиты информации;
- описать расстановку технических средств в помещениях рассматриваемого предприятия.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Общие сведения о защищаемой организации

Наименование организации: ООО «Не по ГОСТу»

Логотип:



Рисунок 1 – Логотип организации

Область деятельности: выполнение функций реализации розничной продукции.

Основные процессы:

- работа с ассортиментом;
- складские операции;
- обработка заказов;
- техническая поддержка.

Информация ограниченного доступа организации:

- коммерческая тайна;
- персональные данные;
- государственная тайна.

1.2 Законодательство в области защиты информации

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Постановление Правительства РФ от 22.11.2012 N 1205 «Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны»;
- Федеральный закон от 28.12.2010 N 390-ФЗ «О безопасности»;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;
- Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011г. «О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними».

2 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

2.1 Общие сведения о технических каналах утечки информации

Утечка информации — это неконтролируемое распространение информации за пределы организации, помещения, здания, какой-либо территории, а также определенного круга лиц, которые имеют доступ к этой информации.

В случае обнаружения утечки важно своевременно ее ликвидировать, но лучше всего заранее принять превентивные меры по защите информации с ограниченным доступом.

Существует три формы утечки информации:

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

В работе будет рассмотрена утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) — совокупность источника информации (передатчика), линии связи (физической среды — канал с шумами), по которой распространяется информационный сигнал, и технических средств перехвата информации (приемника).

Утечка (информации) по техническому каналу — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

На рисунке 2 описана структура технического канала утечки информации.

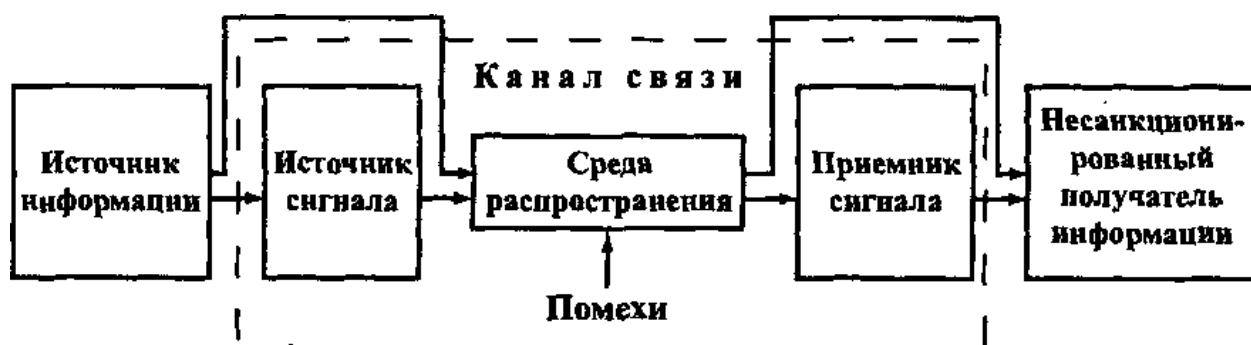


Рисунок 2 — Структура технического канала утечки информации

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника первичного 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, в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.

Передатчик производит преобразование формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Передатчик выполняет следующие функции:

- создает поля или электрический ток, которые переносят информацию;
- производит запись информации на носитель;

- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Обратную функцию передатчика выполняет — приемник. Он производит:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съём информации;
- съём информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Среда распространения сигнала — физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Среда может быть однородная и неоднородная. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую. Однородная — воздух, вода, металл и т.д.

Основными параметрами среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

2.2 Описание технических каналов утечки информации

На рисунке 3 описана классификация технических каналов утечки информации.



Рисунок 3 — Классификация технических каналов утечки информации

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. Поэтому ТКУИ в основном определяют по следующим признаками:

- Оптические. Производится перехват видовой информации с помощью оптических приборов.
- Радиоэлектронные. В этих каналах средой переноса сигналов бывает электрический ток или электромагнитные поля с частотами в радиодиапазоне.
- Акустические. Появление подобного технического канала связано с передачей звуковых сигналов и возникновением колебаний в различных средах под воздействием звуковых волн.
- Материально-вещественные. Источниками информации становятся материальные объекты, выносимые за пределы рабочей зоны.

2.2.1 Оптические каналы утечки информации

Характеристики любого технического канала утечки информации предусматривают наличие трех элементов: объекта наблюдения, среды, по которой распространяется сигнал и устройства приема информации. Для оптического канала объектом станет текст, рисунок, чертеж, изображение на мониторе, прибор. Распространяется оптический сигнал в воздушной среде, по оптическим каналам связи, в безвоздушной среде — космосе — при фотографировании и наблюдении со спутника. На длину канала утечки влияют свойства среды распространения — прозрачность и спектральные характеристики.

При проведении считывания данных с оптических каналов утечки происходит реализация трех функций:

- обнаружение, выявление объекта с еще неизвестными характеристиками;
- различение — выявление крупных деталей, логическое разделение сложных — объектов на элементы;
- опознавание — полный захват значимых характеристик.

В таблице 1 приведены варианты оптических каналов утечки информации.

Таблица 1 — Варианты оптических каналов утечки

Объект	Среда распространения	Приемник
Человек, который находится в помещении	Воздух	Глаза и бинокль
На открытом пространстве	Воздух и стекло	Аппаратура для слежения

Эффективность выявления объекта при наблюдении с помощью глаз или оптических приборов зависит от:

- яркости освещения текста, человека или оборудования;

- резкости контраста между объектом и фоном;
- состояния воздушной среды, от ясного дня до смога или тумана, затрудняющего фиксацию объекта;
- зашумленности изображения, иногда создаваемой специальными средствами маскировки;
- величины объекта. Интересно, что при его увеличении всего в два раза в процессе поиска на открытом пространстве, например, при осмотре видеоискателем поля или площади, скорость выявления искомого увеличится в 8 раз;
- времени наблюдения;
- скорости изменения характеристик, например, скорости движения или чтения страниц текста на экране монитора.

2.2.2 Радиоэлектронные каналы утечки информации

В случае радиоэлектронного канала утечки, носителями выступают магнитные, электрические, электромагнитные поля диапазона, и электрическая энергия, которую распространяют металлические провода. Этот канал обычно используют, чтобы передавать информацию, которую улавливает микрофон специальному приемнику. На этом принципе работает большинство современных спецсредств (жучки — радиомикрофонами или радиостетоскопами). Также, причина утечки информации может крыться и в самом радиоэлектронном канале. Это можно отнести к абсолютно всем возможным средствам связи, начиная с радиостанций и заканчивая мобильными телефонами.

Серьезную угрозу представляет современная оргтехника. Точнее не сама техника, а электромагнитные излучения, которые возникают как побочный продукт при обработке информации. Проблема в том, что обычно эти излучения промодулированы информацией, во время обработки которой они возникли. То есть, если неподалеку от компьютера разместить специальный радиоприемник и портативный компьютер, они будут

улавливать всю информацию, которую обрабатывал компьютер, фиксировать и впоследствии смогут воспроизвести ее.

2.2.3 Акустические каналы утечки информации

Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по телефону;
- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;
- приемника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Перехват акустической информации может происходить не только в помещении или в транспорте, существуют риски утечки даже при разговоре на улице. Шум оживленной трассы или включение воды в номере гостиницы не подавят сигнал, нужны специальные устройства, снижающие риск передачи данных в воздушной среде по каналам утечки акустической информации.

Среди актуальных для большинства организаций носителей угрозы оказываются работники, которые могут быть подкуплены конкурентами:

- сотрудники строительных или ремонтных компаний, присутствующие в помещении при ремонте;
- технический персонал — уборщики, охранники, имеющие допуск в помещение в нерабочие часы;
- настройщики оборудования и приглашенные ИТ-специалисты.

Существует 8 способов перехвата информации при помощи акустических каналов утечки:

- через закладное устройство, спрятанное в помещении;
- по мобильному телефону сотрудника, к которому удаленно подключился злоумышленник;

- через принесенный посетителем диктофон;
- по телефонной линии и сетям 220 В;
- через стекла кабинета и переговорных;
- с помощью компьютера, в котором удаленно активизирован микрофон;
- посредством видеокамеры;
- через строительные устройства и коммуникации ЖКХ, к которым подключен микрофон-стетоскоп.

2.2.4 Материально-вещественные каналы утечки информации

Особенность материально-вещественного канала утечки информации состоит в том, что его наличие позволяет получать секретные сведения, находясь за пределами предприятия. Для получения информации изучаются внешние признаки объектов, физические и химические свойства твердых, газообразных и жидких веществ, случайно попадающих в окружающую среду с территории производства.

В структуру канала, по которому происходит утечка информации, входят:

- Источники данных;
- Линии физического перемещения носителей информации по каналу (людей или вещественных объектов);
- Технические средства перехвата информационных сигналов.
- О деятельности предприятия судят по так называемым «демаскирующим признакам», которые обнаруживаются с помощью специальных средств и приборов.
- Демаскирующие признаки подразделяют на следующие группы:
- Видовые (цвет, структура поверхности, форма предметов);
- Сигнальные (параметры излучений: мощность, амплитуда, диапазон);

- Вещественные (ими являются физические и химические характеристики объектов).

Для получения конфиденциальных данных по таким каналам утечки информации злоумышленники используют прямые и косвенные демаскирующие признаки объектов. Источниками информации в данном случае служат:

- Элементы бракованной продукции, не отправленные на утилизацию;

- Макеты оборудования, черновики записей, сделанных при проведении опытов, разработке планов и проектов. Не уничтоженные вовремя объекты с важной информацией могут попадать в мусорные контейнеры, вывозимые за территорию предприятия;

- Забракованные копии рабочих документов, копировальная бумага и другие отходы делопроизводства, оказавшиеся в корзине для мусора;

- Испорченные электронные носители информации, дефектные жесткие диски компьютеров, вывозимые на мусорные свалки, расположенные за территорией предприятия;

- Твердые, жидкие и газообразные отходы производства, утилизированные не по правилам;

- Радиоактивные отходы.

Нередко подобные объекты важной информации попадают за пределы предприятия по вине сотрудников и посетителей, незнакомых с правилами конфиденциальности.

Методы получения информации с использованием вещественных каналов:

- Химический анализ;

- Биологический анализ;

- Физическое и физико-химические методы.

3 ИССЛЕДОВАНИЕ ПОМЕЩЕНИЙ ПРЕДПРИЯТИЯ

3.1 Обоснование необходимости защиты информации

Объектом защиты является офис интернет-магазина «Не по ГОСТу», который занимается продажей товаров с военной атрибутикой, товаров для военнослужащих

Согласно Постановлению Правительства РФ от 06.02.2010 N 63 (ред. от 29.10.2022) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Постановлению Правительства РФ от 23.08.2018 N 984 «Об утверждении Правил подтверждения степени секретности сведений, с которыми предприятия, учреждения и организации предполагают проводить работы, связанные с использованием сведений, составляющих государственную тайну», а также ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 N 44-ФЗ, у руководителей негосударственных организаций, планирующих участие в закупке товаров для обеспечения государственных нужд с использованием сведений, составляющих государственную тайну, есть допуск третьей формы — для граждан, допускаемых к секретным сведениям. Соответственно, в целом наивысшим уровнем секретности для предприятий данного типа является уровень «секретно».

3.2 План и описание помещений предприятия

На рисунке 4 представлен план помещения, рассматриваемого в этой работе.

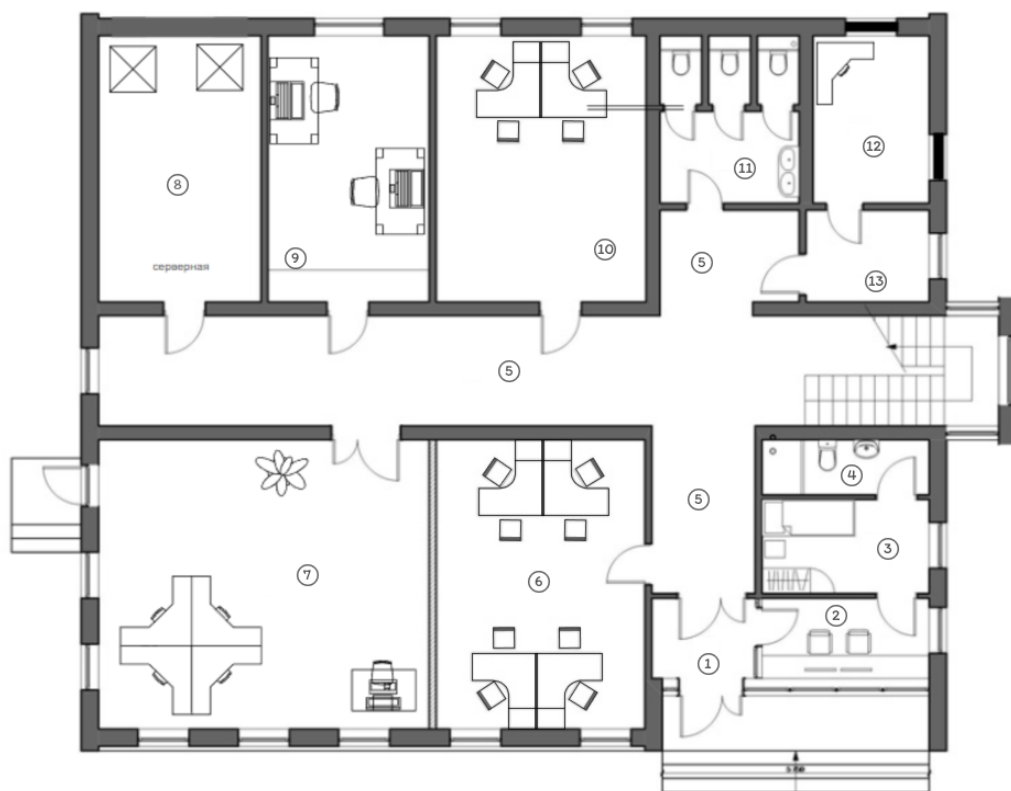


Рисунок 4 — План помещений до установки ТСЗИ

Легенда:

1. Досмотровая комната
2. Пост охраны
3. Комната отдыха охраны
4. Санузел охраны
5. Общая зона
6. Кабинет
7. Общий кабинет
8. Серверная
9. Кабинет
10. Кабинет
11. Санузел общий
12. Кабинет директора
13. Комната ожидания

На рисунке 5 показана схема информационных потоков в рассматриваемом предприятии.

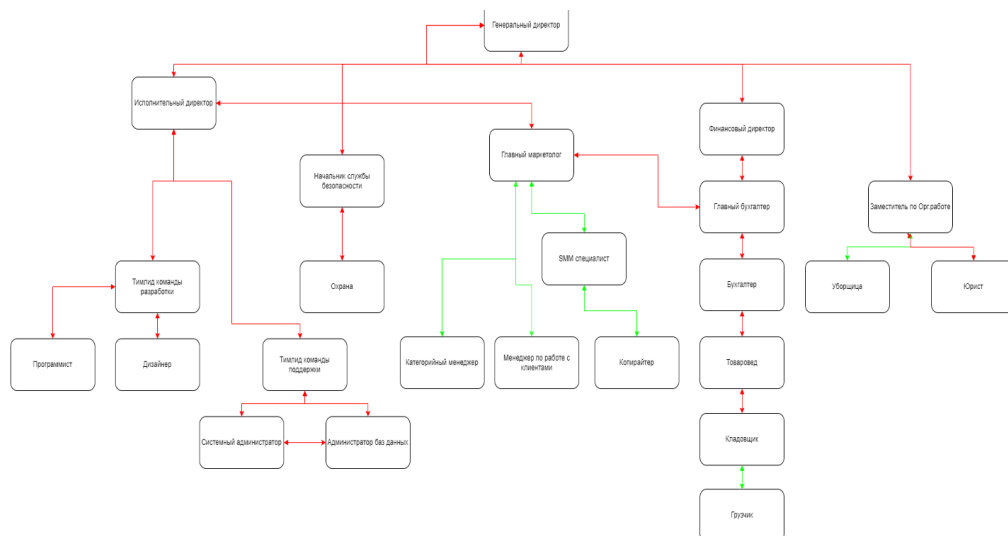


Рисунок 5 — Схема информационных потоков

Рассматриваемые помещения имеют следующую площадь:

1. Досмотровая комната — 12 м^2
2. Пост охраны — 5 м^2
3. Комната отдыха охраны — 10 м^2
4. Санузел охраны — $4,5 \text{ м}^2$
5. Общая зона + лестничная площадка — $61,9 \text{ м}^2$
6. Кабинет — 25 м^2
7. Общий Кабинет — 40 м^2
8. Серверная — 20 м^2
9. Кабинет — 20 м^2
10. Кабинет — 25 м^2
11. Санузел общий — $10,5 \text{ м}^2$
12. Кабинет директора — $9,5 \text{ м}^2$

13. Комната ожидания — 5 м²

3.3 Анализ возможных утечек информации

Каналы утечек информации обычно классифицируют как косвенные и прямые. В нашем случае, могут быть следующие утечки информации по косвенным каналам:

- поиск конфиденциальных данных при исследовании мусора, выброшенных документов и т.д.: в здании имеются санузлы и мусорки в кабинетах.
- потеря или преднамеренная кража флеш-носителя: сотрудники могут хранить свои флеш-носители на рабочих местах.
- считывание побочных электромагнитных излучений и наводок: в каждом помещении находятся розетки, которые являются не только электромагнитным каналом утечки, но и электрическим.
- попытка кражи информации за счет оптических средств: почти в каждом помещении есть окна, поэтому есть вероятность фотографирования объектов информации или прослушивание помещений.

Когда речь идет про прямые каналы утечек информации, то имеют в виду, что злоумышленник имеет доступ к аппаратному обеспечению и информации, которая используется в информационной системе. В нашем случае могут быть следующие утечки по прямым каналам:

- копирование информации: сотрудники могут преднамеренно или непреднамеренно скопировать конфиденциальную информацию;
- работа инсайдеров: сотрудники преднамеренно (сами устраиваются в компанию, чтобы вынести важную информацию) или непреднамеренно (стали жертвой и раскрыли информацию в неформальной обстановке) могут раскрыть информацию.

Для защиты данных в компаниях важно учесть технические каналы утечки.

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.

К пассивным техническим способам защиты относят: установка комплексных систем защиты от несанкционированного доступа (НСД) на ТСПИ и кабельные линии связи, экранирование ВП, ТСПИ и отходящих от них соединительных линий.

Ниже в таблице 2 приведены средства защиты информации, необходимые для обеспечения комплексной безопасности согласно типа информации — государственная тайна уровня «секретно».

Таблица 2 — Каналы утечек

Каналы	Источники	Пассивная защита	Активная защита
Оптический	Двери и окна	Шторы или жалюзи, доводчики на дверях для плотного закрывания дверей, тонирующие пленки на окна	Блокирующие устройства
Вибрационный и виброакустический	Батареи или другие твердые поверхности	Обшивка стен, которые способствуют изолированию звука и вибрации	Устройства вибрационного шумления
Акустический и акустоэлектрический	Двери, окна, проводка	Фильтры для сетей электропитания, звукоизоляция помещений	Устройства акустического шумления
Электромагнитный и электрический	Розетки, АРМы, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного шумления

4 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ РАССМАТРИВАЕМОГО ПРЕДПРИЯТИЯ

4.1 Анализ рынка технических средств

4.1.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- усиленные двери;
- тамбурное помещение перед некоторыми помещениями;
- дополнительная отделка кабинетов звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления. Ниже в таблице 3 представлен сравнительный анализ рассматриваемых средств.

Таблица 3 — Системы акустического и виброакустического зашумления

Критерии\модель	Камертон-5	Соната-АВ модель 3М	Барон-S1	Буран
Диапазон частот	90-11200 Гц	90-11200 Гц	60-16000 Гц	100-11200 Гц
Количество подключаемых излучателей	до 96	до 65	до 2	до 50
Количество каналов	4	3	2	3
Соответствие требованиям документов	Соответствует требованиям 1 класса защищенности	Соответствует требованиям 1 класса защищенности	Соответствует требованиям 1 класса защищенности	Соответствует требованиям 2 класса защищенности
Стоимость	46000	18000	33500	67500

По результатам анализа была выбрана системы Соната-АВ модель 4Б. Из рассматриваемых моделей, Соната-АВ имеет наименьшую стоимость, возможность индивидуальной регулировки интегрального уровня и корректировки спектра каждого генератора.

4.1.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях здания.

Активная защита основывается на создании в сети белого шума, которые скрывает колебания порождаемые воздействием звуковой волны или работающей электрической техникой.

В таблице 4 представлен сравнительный анализ подходящих средств активной защиты.

Таблица 4 — Системы шумления против электрического канала

Критерии\модель	ЛГШ-513	ЛГШ-221	Соната-РС2
Диапазон частот	90-11200 Гц	90-11200 Гц	60-16000 Гц
Диапазон регулировки шума	не менее 20 дБ	не менее 20 дБ	не менее 20 дБ
Потребляемая мощность	Не более 45 ВА	Не более 45 ВА	Не более 10 Вт
Соответствие требованиям документов	Соответствует требованиям 2 класса защищенности	Соответствует требованиям 2 класса защищенности	Соответствует требованиям 1 класса защищенности
Стоимость	39000	36400	32400

В результате анализа было выбрано средство ЛГШ-513. Одним из важных факторов выбора, являлось то, что это средство также относится к защите от ПЭМИН. Также оно имеет наиболее широкий спектр и защищает от электрического и электромагнитного каналов.

4.1.3 Устройства для перекрытия утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН)

Для защиты от ПЭМИН следует использовать генераторы шума в помещениях, в которых установлены средства конфиденциальной информации.

В результате анализа, описанного в пункте 4.1.2, было выбрано средство ЛГШ-513 так как оно не только способствует перекрытию электрического и электромагнитного каналов утечки информации, но и защищает от ПЭМИН. Данный выбор также обоснован тем, что устройство имеет подключения проводного дистанционного управления и контроля.

4.1.4 Устройства для перекрытия оптического канала утечки информации

В качестве защиты от утечки информации по оптическому каналу достаточно будет ликвидировать оптические контакт. Для этого стоит снизить освещенность защищаемого объекта, закрыть окна кабинетов шторами, тонированными пленками, ширмами и применить специальную маскировку и средства сокрытия, такие как сетки, аэрозольные завесы, краски.

Оптимальным решением для защиты окон будет установка штор или жалюзи, а для защиты дверей установка доводчика, для плотного закрытия.

4.2 Описание расстановки технических средств

Выбранные средства:

- система виброакустической и акустической защиты Соната АВ модель 3М;
- генератор шума ЛГШ-512;
- доводчики на двери;
- усиленные двери, обшитые металлом со звукоизолирующей прокладкой на металлическом каркасе: кабинет директора, выход и выход из тамбура у охраны, кабинет охраны, серверная, дверь на улицу из общего кабинета, вход в общий кабинет;
- тамбурное помещение перед кабинетом директора;
- жалюзи на окна.

Согласно руководству по эксплуатации системы Соната «АВ», оптимальное количество излучателей для каждого помещения определяется такими факторами, как его конструкция, материалы ограждающих поверхностей, расположение помещения, уровень шумового фона и т.п.

Для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

- при зашумлении массивных стен использовать один виброизлучатель ВИ-3М (ВИ-45) на каждые $15...25 \text{ м}^2$ площади поверхности стены (при этом излучатели должны устанавливаться на уровне половины высоты стены при высоте стены менее 5 м или на высоте от пола помещения не менее 2.5 м при высоте стены 5 м и более, далее – через каждые 5 м высоты);
- при зашумлении потолка (пола) — один виброизлучатель ВИ-3М (ВИ-45) на каждые $15...25 \text{ м}^2$ перекрытия;
- при зашумлении окна — один виброизлучатель ВИ-3М (ВИ-45) на каждое окно или отдельную раму или один пьезоизлучатель ПИ-3М (ПИ-45) на каждый элемент остекления;

- при зашумлении двери — один виброизлучатель ВИ-3М (ВИ-45) на каждое полотно двери;
- при зашумлении трубы систем водо-, тепло- или газоснабжения — один виброизлучатель ВИ-3М (ВИ-45) на каждую отдельную трубу;
- при зашумлении вентиляционных каналов, дверных тамбуров, смежных помещений — один аудиоизлучатель АИ-3М (АИ-65) на каждый вентиляционный канал, дверной тамбур или входную дверь, смежное помещение;
- при зашумлении надпотолочного пространства или других пустот — один аудиоизлучатель АИ-3м (АИ-65) на каждые $8...12 \text{ м}^2$ надпотолочного пространства или других пустот.

Итого будет установлено:

- виброизлучатель ВИ-45 или ПИ-45 на окна;
- виброизлучатель ВИ-45 на стены;
- виброизлучатель ВИ-45 на двери;
- виброизлучатель ВИ-45 на пол и потолки;
- виброизлучатель АИ-65 для вентиляции, смежных помещений;
- виброизлучатель АИ-65 для надпотолочного пространства.

4.3 План помещения с активной и пассивной защитой

На рисунке 6 описаны все условные обозначения устройств, которые были размещены на плане помещения.

	Аудиоизлучатель АИ-3М на дверной тамбур
	Размыкатель слаботочных линий Соната-ВК4.2
	ЛГШ-513 — перекрытие электрического, акустоэлектрического и электромагнитного каналов + защита от ПЭМИН
	Виброизлучатель ВИ-45 на двери
	Доводчик двери
	Виброизлучатель ВИ-45 на стену
	Виброизлучатель ВИ-45 на пол
	Виброизлучатель ВИ-45 на окно/батарею
	Виброизлучатель ВИ-45 на потолок
	Размыкатель интернет линий Соната ВК4.3
	Отделка помещений звукоизолирующими материалами
	Усиленные звукоизолирующие двери

Рисунок 6 — Условные обозначения

На рисунке 6 представлены условные обозначения инженерно-технических средств защиты информации.

На рисунке 7 представлен план с размещенными устройствами пассивной и активной защиты.



Рисунок 7 — План помещения с активной и пассивной защитой

ЗАКЛЮЧЕНИЕ

В результате выполнения работы был проведен теоретический анализ технических каналов утечки информации, анализ выбранного предприятия и обрабатываемой там информации, рынка инженерно-технических средств защиты информации, а также выполнено проектирование инженерно-технической системы защиты информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 04.08.2023) // Собрание Законодательства Российской Федерации.
2. Системы виброакустической и акустической защиты «СОНАТА-АВ» Модель 3М // Руководство по эксплуатации.
3. Утечка информации [Электронный ресурс]. — URL: <https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/> (дата обращения 07.12.2023).
4. Каналы утечки информации [Электронный ресурс]. — URL: https://xn--80aidjgwzd.xn--p1ai/news/kanaly_utechki_informatsii_v_kompanii/ (дата обращения 08.12.2023)
5. Каналы утечки конфиденциальной информации [Электронный ресурс]. — URL: <https://www.podavitel.ru/kanali-utechki-informacii.html>