

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

**«Организация и управление службой
информационной безопасности»**

На тему:

**«Проектирование инженерно-технической защиты
информации на предприятии. Вариант 7.»**

Выполнил:

Студент группы N34461
Могиленко Никита
Вячеславович

Проверил преподаватель:

Попов И. Ю.,
К. Т. Н.,
доцент ФБИТ

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Могиленко Н.В. (Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 (Технологии защиты информации)
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 защиты информации на предприятии
Задание	проанализировать мотивации и угрозы, которые внешние нарушители используют для достижения своих целей, а также меры защиты от внешних нарушителей информационной безопасности

Краткие методические указания

Подготовить отчет по курсовой работе по образцу и презентацию для защиты.

Содержание пояснительной записки

Курсовая работа содержит введение, организационную структуру предприятия, обоснование защиты информации, описание помещения, анализ рынка технических средств, рекомендации по организации защиты, заключение, список источников.

Рекомендуемая литература

Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности Учебное пособие / СПб: НИУ ИТМО, 2013-148с

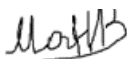
Руководитель	_____ (Подпись, дата)
Студент	 27 октября 2023 (Подпись, дата)

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

(Фамилия И.О.)

Группа N34461

Руководитель Попов И. Ю., к. т. н., доцент ФБИТ

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

Наименование темы	Проектирование инженерно-технической защиты информации на предприятии
--------------------------	---

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение титульных листов и поиск источников	29.09.2023	30.09.2023	
2	Анализ информации	29.09.2023	30.09.2023	
3	Написание курсовой работы	14.10.2023	14.10.2023	
4	Подготовка презентации	21.10.2023	21.10.2023	
5	Защита курсовой работы	28.10.2023	28.10.2023	

(Подпись, дата)

Maths

27 октября 2023

(Подпись, дата)

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

Студент Могиленко Н.В.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

Направление (специальность) 10.03.01 (Технологии защиты информации)

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 защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА
(РАБОТЫ)**

**1. Цель и задачи
работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

**2. Характер
работы**

☐ Расчет

☐

☐ Моделирование

Конструирование

Другое: Исследовательская работа

3. Содержание работы

1. Введение.
2. Анализ организационной структуры предприятия.
3. Требования к системе защиты информации
4. Анализ защищаемых помещений.
5. Анализ рынка инженерно-технических средств.
6. Размещение инженерно-технических средств защиты
7. Заключение.
8. Список использованных источников.

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки

информации в предложенных помещениях, предложены меры пассивной и активной

Руководитель

(Подпись, дата)

Студент



27 октября 2023

(Подпись, дата)

«27» октября 2023 г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
1 АНАЛИЗ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ	8
1.1 ИЗУЧЕНИЕ ОСОБЕННОСТЕЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ, ЕГО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ПОТОКОВ	8
1.2 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	12
1.2.1 СХЕМА ПОМЕЩЕНИЯ	12
1.2.2 АНАЛИЗ ВОЗМОЖНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	15
2 ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ	16
2.1 ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ТРЕБОВАНИЙ, ПРЕДЪЯВЛЯЕМЫХ К ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ.....	16
3 АНАЛИЗ РЫНКА ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ	18
3.1 ОПРЕДЕЛЕНИЕ СРЕДСТВ ЗАЩИТЫ.....	19
3.1.1 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРОАКУСТИЧЕСКИМ КАНАЛАМ.....	19
3.1.2 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРИЧЕСКИМ, АКУСТОЭЛЕКТРИЧЕСКИМ И ЭЛЕКТРОМАГНИТНЫМ КАНАЛАМ.....	22
3.1.3 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ.....	26
4 РАЗМЕЩЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ.....	27
5 ЗАКЛЮЧЕНИЕ.....	31
6 Список использованной литературы	32

ВВЕДЕНИЕ

В современном информационном обществе, где информация является ключевым ресурсом предприятий, обеспечение ее безопасности становится приоритетной задачей. Развитие информационных технологий и расширение возможностей в сфере электронных коммуникаций предоставляют предприятиям множество преимуществ, но также подвергают их информационные ресурсы новым и неизбежным угрозам.

Цель данной курсовой работы состоит в разработке и проектировании инженерно-технической системы защиты информации на предприятии. Эта система направлена на обеспечение конфиденциальности, целостности и доступности информации, а также минимизацию рисков, связанных с возможными угрозами информационной безопасности.

Актуальность темы обусловлена не только постоянным ростом угроз в сфере информационной безопасности, но и увеличением объемов обрабатываемой и хранимой информации на предприятии. Каждый эпизод нарушения безопасности может привести к серьезным последствиям, включая утечку конфиденциальных данных, финансовые потери и потерю доверия со стороны клиентов и партнеров.

В рамках курсовой работы будет проведен анализ существующей информационной инфраструктуры предприятия, а также предложены и реализованы эффективные меры по защите информации. Проектирование инженерно-технической системы защиты информации будет ориентировано на учет специфики бизнес-процессов предприятия и обеспечение комплексного подхода к обеспечению безопасности.

Всестороннее исследование и разработка данной системы представляют собой важный этап в повышении общей устойчивости предприятия к современным угрозам в области информационной безопасности.

1 АНАЛИЗ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ

Название организация: неклассическая компания "SOK". SOK является неклассической компанией специализирующейся в разработке и внедрении передовых технологий в области информационных технологий, искусственного интеллекта и кибербезопасности. SOK предоставляет клиентам передовые решения и обеспечивает безопасность и консультации в сфере информационных технологий.

Часть разрабатываемых проектов, происходит в сотрудничестве с государственными компаниями. В частности, связанных со сведениями, составляющими государственную тайну уровня “совершенно секретно”. Как следствие, необходимо оборудовать офисное помещение инженерно-техническими средствами защиты информации.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

1.1 ИЗУЧЕНИЕ ОСОБЕННОСТЕЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ, ЕГО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ПОТОКОВ

Основные функции Организации:

- Проведение исследований в области новейших технологий, создание инновационных решений и разработка прототипов.
- Предоставление консультаций по внедрению новых технологий, обучение персонала клиентов и партнеров.
- Проведение аудитов безопасности, разработка средств защиты информации и обеспечение кибербезопасности для корпоративных клиентов.
- Установление стратегических партнерств с ведущими технологическими компаниями для обмена знаниями и ресурсами.

Основные должности, имеющиеся в организации, а также их обязанности представлены в Таблице 1.

Таблица 1 – Должности и их обязанности в Организации

Должность	Обязанности
Директор	<p>Определение стратегического курса организации. Принятие ключевых решений по развитию и инвестициям.</p> <p>Представление организации перед стейкхолдерами и общественностью.</p>
Менеджер по разработке	<p>Организация и координация исследовательских проектов.</p> <p>Руководство отделом разработки.</p> <p>Взаимодействие с ведущими научными центрами и университетами.</p>
Начальник Безопасности	<p>Проведение аудитов безопасности информационных систем.</p> <p>Разработка и внедрение стратегий киберзащиты.</p>
Специалист ИБ	Мониторинг современных угроз в области кибербезопасности.
Охранник	Обеспечение физической безопасности на территории предприятия.
Разработчик ПО	<p>Проектирование и разработка программных продуктов.</p> <p>Тестирование и оптимизация программного кода.</p> <p>Сотрудничество с другими разработчиками в командной среде.</p>
Системный Администратор	<p>Обеспечение стабильной работы информационных систем.</p>

	Управление сетевой инфраструктурой. Решение технических проблем и поддержка пользователей.
Бухгалтер	Учет и анализ финансов Налоговый учет Соблюдение финансовых стандартов
HR	Поиск и привлечение новых клиентов. Работа с партнерами и развитие бизнес-сети. Участие в разработке бизнес-стратегий. Разработка и реализация маркетинговых стратегий. Продвижение бренда и продуктов организации. Взаимодействие с медиа и создание контента.



Рисунок 1 – Организационная структура предприятия

Информационные потоки в организации представляют собой систему передачи данных и сообщений между различными элементами организационной структуры. Эти потоки играют ключевую роль в обеспечении эффективной коммуникации и

взаимодействия между различными уровнями управления, подразделениями и сотрудниками организации. Информационные потоки могут быть как формальными, так и неформальными.

Рассмотрим основные информационные потоки в Организации. На Рисунке 2 зеленым цветом обозначены открытые потоки, а красным цветом - закрытые потоки.

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

К защищаемой информации, передающейся по закрытым потокам, относятся персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна и сведения о разрабатываемом технологических решений.

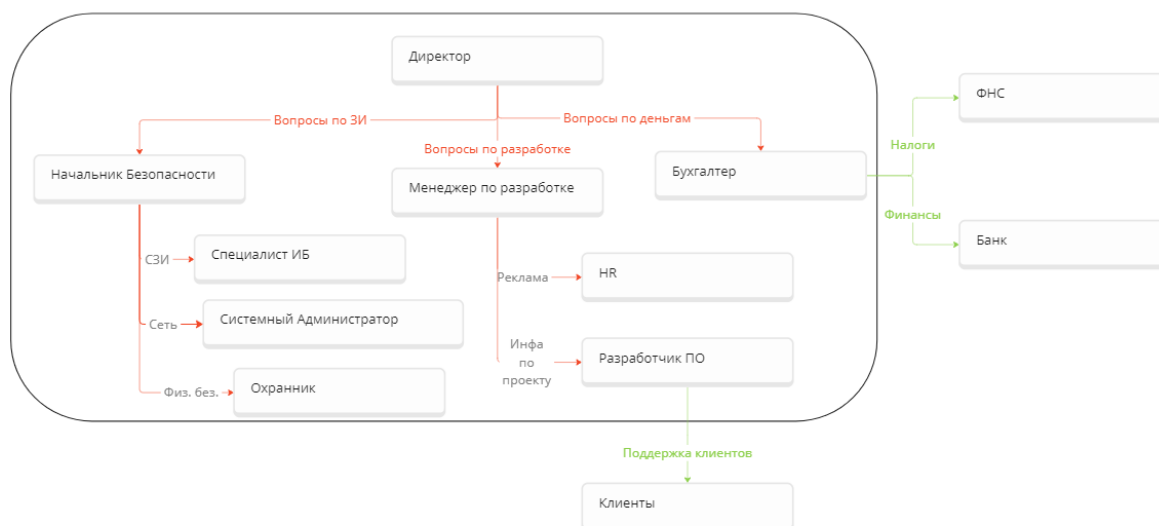


Рисунок 2 – Информационные потоки в Организации

1.2 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

1.2.1 СХЕМА ПОМЕЩЕНИЯ

Защищаемый объект состоит из тринадцати помещений и представляет собой офис предприятия с двумя переговорными, кабинетом директора, раздевалкой, двумя санузлами, кабинетами отдела разработки, главным холлом, серверной и кухней.

На Рисунке 3 и Таблице 2 представлен план защищаемого помещения, а также в Таблице 3 представлена их площадь.

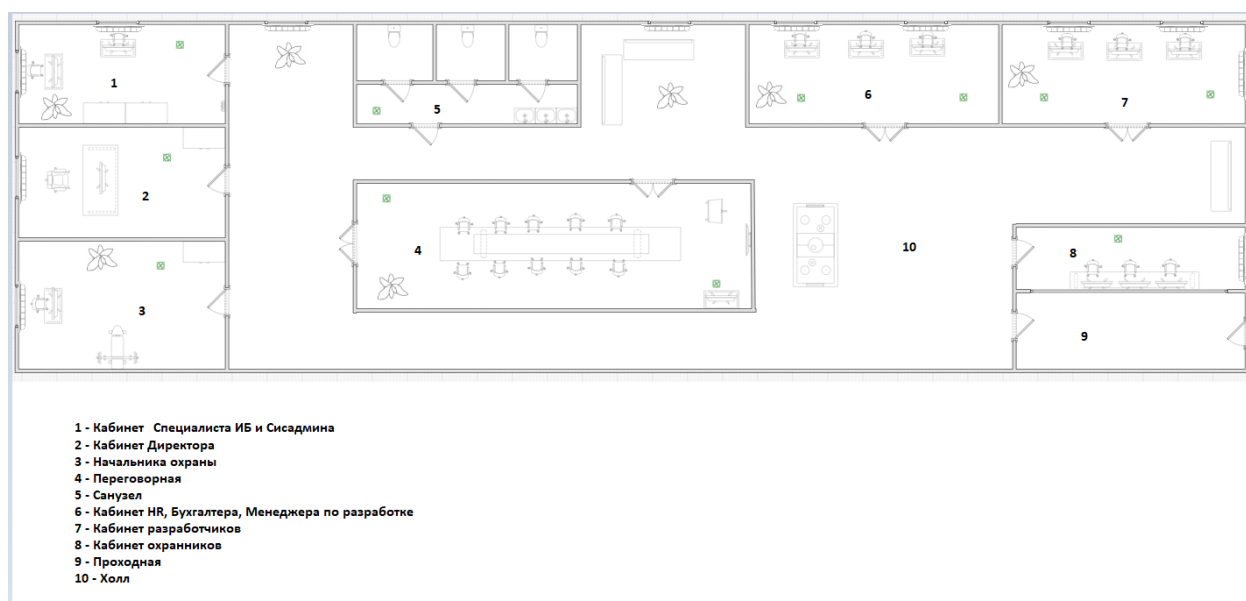


Рисунок 3 – План защищаемого помещения

Таблица 2 – Описание обозначений

Обозначение	Описание
	вентиляция
	Стол с компьютером
	растение
	Батарея отопления
	Шкаф для документации








	Кресло для руководителя
	Кресло сотрудника
	унитаз
	аэрохоккей
	флипчарт
	телевизор
	диван

Таблица 3 – Площадь помещений

Помещение	Площадь, м ²
Кабинет специалиста иб и сисадмина	16.71
Кабинет директора	18.58
Кабинет начальника охраны	21.50
Переговорная	193.69
Санузел	17
Кабинет HR, Бухгалтера, Менеджера по разработке	20.21
Кабинет разработчиков	19.66
Кабинет охранников	11.59
Проходная	14.18
Холл	111.654

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся три дивана, один аэрохоккей, два горшка с растениями, 3 батареи отопления. Оснащен 8 розетками.

В переговорной расположено 8 стульев, стол, телевизор, растение, компьютер, флипчарт.

В кабинете директора расположен шкаф с документами, стул, рабочий стол, компьютер,

В кабинете начальника охраны расположены 1 кресло, 1 рабочий стол, 1 батарея отопления, шкаф, комнатное растение, штанга.

В кабинете разработчиков и исследователей расположены 16 рабочих столов, 16 компьютерных кресел, 3 батареи отопления, мусорное ведро. Оснащено 24 розетками.

В кабинете для работы с гостайной расположены 3 рабочих стола, 3 компьютерных кресел, 3 компьютеров, 3 батареи отопления.

В кабинете разработчиков 3 рабочих стола, 3 компьютерных кресел, 3 компьютеров, 3 батареи отопления.

В кабинете охранников 1 рабочий стол, 3 компьютерных кресел, 3 компьютеров, 1 батарея отопления.

Офис расположен на первом этаже малоэтажного здания, окна выходят в закрытый контролируемый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне.

Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину 10см.

1.2.2 АНАЛИЗ ВОЗМОЖНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В каждом помещении скрываются потенциальные пути для нежелательного раскрытия информации, связанные с возможными электромагнитными и электрическими утечками, такими как использование компьютеров и электрических розеток. Не следует забывать и о декоративных элементах, таких как комнатные растения, картины, скульптуры, которые могут быть использованы для скрытой установки закладных устройств, способных передавать информацию через акустический канал.

Существует также опасность утечки данных через оптические каналы, например, из-за незакрытых окон и недостаточно защищенных дверей.

Следует учесть и влияние виброакустического канала, который может использоваться для передачи информации через твердые поверхности, такие как стены или батареи отопления.

Необходимо также учитывать возможность физического канала утечки информации, связанного с наличием материальных носителей данных. Однако стоит отметить, что этот канал не всегда поддается техническим средствам защиты.

При обеспечении безопасности помещения важно учитывать разнообразные потенциальные пути утечки информации и принимать соответствующие меры для их предотвращения.

2 ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ТРЕБОВАНИЙ, ПРЕДЪЯВЛЯЕМЫХ К ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

При разработке комплекса средств защиты информации будем руководствоваться следующими документами:

- Закон “О государственной тайне”;
- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;
- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне";
- Постановление Правительства РФ от 15 апреля 1995 г. №333 “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”;
- Постановление 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";
- Постановление Правительства РФ от 22.11.2012 N 1205 "Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны";
- «Типовые нормы и правила 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.

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите

государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

- стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см;
- в помещениях для работы с гостайной 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;
- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
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;
- все режимные помещения оборудуются аварийным освещением;
- вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;
- 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.

3 АНАЛИЗ РЫНКА ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к грифу «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в Таблице 4. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 4 – Активная и пассивная защита различных каналов утечки информации

Каналы	Источники	Пассивная защита	Активная защита
Электрический Электромагнитный	АРМ, розетки, иные электрические приборы	Защитные металлические экраны и фильтры для сетей электропитания	Устройства электромагнитного зашумления
Акустический акустоэлектрический	Окна, двери, стены электрическая проводка, вентиляция	Защитные экраны и фильтры для сетей электропитания, звукоизоляция помещений	Устройства акустического зашумления
Оптический	Окна и стеклянные поверхности, двери	Доводчики дверей, средства преграждения отраженного света	Маскирующие устройства, жалюзи, бликующие устройства
Вибрационный, виброакустический	Стекля, стены, батареи отопления и иные твердые поверхности	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов	Устройства вибрационного зашумления

3.1 ОПРЕДЕЛЕНИЕ СРЕДСТВ ЗАЩИТЫ

Существует три категории выделенных помещений (то есть помещений, специально предназначенных для проведения совещаний по вопросам, содержащим сведения, составляющие государственную тайну Российской Федерации):

1 категория — разрешается обсуждать информацию с грифом до «особой важности» включительно;

2 категория — с грифом до «совершенно секретно» включительно;

3 категория — с грифом до «секретно» включительно.

. Для защиты помещения, предназначенного для работы с государственной тайной уровня «совершенно секретно», будут рассмотрены средства активной защиты информации

для выделенных помещений не ниже 2 категории.

3.1.1 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРОАКУСТИЧЕСКИМ КАНАЛАМ

Для пассивной защиты объекта используются следующие средства:

- усиленные звукоизоляционные двери;
- дополнительная отделка переговорной звукоизолирующими материалами.

В качестве средств активной защиты используется система виброакустического шумления. В Таблице 5 приведен сравнительный анализ решений, предлагаемых на современном рынке, и удовлетворяющих указанным требованиям для защиты объекта от утечек по акустическому и виброакустическому каналу.

Таблица 5 – Средства защиты от утечки по акустическим и виброакустическим каналам

Модель	Характеристики	Особенности	Цена, руб.
ЛГШ-404	<p>Диапазон рабочих частот 175...11200 Гц</p> <p>Потребляемая мощность 25 Вт</p> <p>Электропитание 220 В, 50 Гц</p> <p>Габаритные размеры генераторного блока 188х160х60 мм</p> <p>Количество подключаемых излучателей на канал до 20 шт.</p>	<p>Сертификат ФСТЭК</p> <p>Генератор шума ЛГШ-404 (генераторный блок с 2 выходами);</p> <p>вибровозбудители ЛВП-10 для установки на стекла, межкомнатные перегородки, трубы инженерных коммуникаций; акустические излучатели ЛВП-2А, создающие маскирующие помехи в дверных проемах, вентиляционных воздуховодах и в прочих закрытых пространствах;</p> <p>виброэкраны ЛИСТ-1 для установки на окна</p>	35 100
Соната «АВ» модель 4Б	<p>Диапазон рабочих частот 90...11200 Гц</p> <p>Потребляемая мощность до 40 Вт</p> <p>Электропитание 220 В, 50 Гц</p> <p>Габариты блока, не более 142х60х167 мм</p>	<p>Сертификат ФСТЭК</p> <p>Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа</p> <p>Индивидуальная регулировка интегрального уровня и корректировка спектра каждого</p>	44 200

	<p>Количество подключаемых излучателей на канал до 239 шт.</p>	<p>генератора улучшает действие системы</p> <p>Позволяет создать систему автоматического контроля всех элементов, снизить время на конфигурирование и тестирование системы</p> <p>Изменить настройки генераторов и построить гибкую систему виброакустической защиты, уменьшить затраты благодаря использованию единой линии связи и электропитания</p>	
«Барон»	<p>Диапазон частот 150 Гц...15кГц</p> <p>Количество выходных каналов: 4</p> <p>Потребляемая мощность: 15 Вт на канал</p> <p>Электропитание 220 В, 50 Гц.</p> <p>Дальность действия дистанционного управления: 30 м</p>	<p>Полностью цифровое управление;</p> <p>интеллектуальное меню, гибкая система конфигурирования;</p> <p>возможность формирования помехового сигнала от различных внутренних и внешних источников и их комбинаций</p> <p>наличие четырех независимых выходных каналов с отдельными регулировками для оптимальной настройки помехового сигнала для различных защищаемых поверхностей и каналов утечки</p>	53 300

Исходя из анализа, представленного в Таблице 5, было принято решение о выборе системы «Соната АВ-4Б». По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов. Особенностью «Соната АВ-4Б» является использование принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что обеспечивает высокую степень надежности в защите информации.

Кроме того, усовершенствованная настройка аппаратных элементов модели 4Б позволяет интегрировать источник электропитания с другими для обмена информацией. Соната АВ-4Б содержит генераторы-акустоизлучатели СА-4Б и генераторы-вибровозбудители СВ-4Б, блок электропитания и управления Соната ИП-4.3 и пульт управления Соната ДУ-4.3.

Также данный комплекс защиты необходимо дополнить размыкателем телефонной линии «Соната-ВК4.1», размыкатель слаботочной линии «Соната-ВК4.2» и размыкатель линии Ethernet «Соната-ВК4.3».

3.1.2 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРИЧЕСКИМ, АКУСТОЭЛЕКТРИЧЕСКИМ И ЭЛЕКТРОМАГНИТНЫМ КАНАЛАМ

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в Таблице 6.

Таблица 6 – Активная защита от утечек информации по электрическим, акустоэлектрическим и электромагнитным каналам

Модель	Характеристики	Особенности	Цена, руб.
ЛГШ-221	Диапазон частот 10 кГц – 400 МГц. Диапазон	Сетевой генератор шума. Устройство оснащено световым и звуковым	36 400

	<p>регулировки уровня выходного шумового сигнала не менее 20 дБ. Мощность, потребляемая от сети не более 45 ВА.</p>	<p>индикаторами работы. Возможность управления устройством с помощью пульта ДУ.</p>	
Соната-РСЗ	<p>Тип индикации: светодиодная/ звуковая Работа от сети ~220 В +10%/-15%, Частота 50 Гц. Потребляемая мощность – 10Вт. Продолжительность работы не менее 8 часов.</p>	<p>Сертификат ФСТЭК Возможно дистанционное управление посредством проводного пульта. 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.</p>	32 400

Соната- РС1	<p>Диапазон частот до 1</p> <p>ГГц, регулировка уровня шума в 1 частотной полосе.</p> <p>Напряжение 220 В.</p>	<p>Сертификат ФСТЭК</p> <p>Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)</p>	16 520
Соната-РЗ.1	<p>Виды индикации:</p> <p>Световая/звуковая</p> <p>Диапазон частот: 0.01...100 МГц</p> <p>Электропитание: 220 В +10%/-15%, Частота 50 Гц</p> <p>Потребляемая мощность: 10 Вт</p> <p>Продолжительность работы: не менее 8 часов</p> <p>Длина шнура: 2 м</p>	<p>Сертификат ФСТЭК</p> <p>Может применяться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления); наличие регулятора интегрального уровня формируемых</p>	33 120

		<p>электромагнитного поля шума и шумовых напряжений; за счет применения опционально поставляемой дополнительной антенны; встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией; возможность удаленного управления изделием наличие счетчика наработки в режиме «Излучение».</p>	
--	--	--	--

В результате сравнения в качестве применяемого решения было выбрано средство активной защиты информации "Соната-РЗ.1". Кроме того, оно может применяться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации.

Дополнительным фактором выбора именно данного устройства является тот же производитель, что дает нам возможность встроить его в систему «Соната АВ-4Б», выбранную нами в предыдущем пункте задания.

3.1.3 СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ

Для обеспечения защиты помещения от возможной фото-видеосъемки или визуального наблюдения следует установить жалюзи/шторы на окна и также воспользоваться доводчиками для дверей. Выбранные шторы и доводчики, а также двери представлены в Таблице 7.

Таблица 7 – Защита от утечек по оптическим каналам

Модель	Характеристики	Особенности	Цена, руб.
Шторы «Inspire Miami»	Размер 200x280 см Цвет: черный	Штора на ленте со скрытыми петлями	3 798
Дверь звукоизоляционная усиленная «SWEDOOR»	Цвет: черный толщина дверного полотна гладкой двери 40 мм Звукоизоляция Rw 30 дБ, что соответствует классу звукоизоляции 25 дБ	Дверное полотно с фальцем, уплотнитель по периметру;	87 711
Доводчик Geze TS-1500 EN3-4	Морозостойкие, внутренние, двухскоростные, рельсовые Усилие закрывания EN3-4 (от 60кг до 120 кг) Максимальная ширина створки 1100 мм	Регулируемая скорость закрывания Регулируемый гидравлический дожим в конечном 15-градусном секторе закрывания	3 740

4 РАЗМЕЩЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

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

- комплекс виброакустической защиты помещения «Соната АВ-4Б»;
- ПЭМИН «Соната-РЗ.1»
- жалюзи на семь окон;
- 5 усиленных дверей с толщиной 40 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

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

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

- стены – один на каждые 3-5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15-25 м² перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

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

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

В Таблице 8 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 8 – Расчетная таблица стоимости средств защиты

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
-------------	------------	-----------------	--------------------

Блок электропитания и управления «Соната-ИП 4.3»	21 600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б»	3 540	11	38940
Генератор-вибровозбудитель «Соната СВ-4Б»	7 440	30	223200
Размыкатель телефонной линии «Соната ВК4.1»	6 000	1	6 000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Размыкатель линии Ethernet «Соната ВК4.3»	6 000	1	6 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
ПЭМИН «Соната-Р3.1»	33 120	8	264960
Шторы Blackout «Inspire Miami»	3 798	10	37980
Усиленные звукоизолирующие двери «SWEDOOR»	87 711	5	438555
Доводчик Geze TS-1500 EN3-4	3 740	5	18700
Итого:			1069615

В пяти помещениях установлены усиленные звукоизолирующие двери, как показано на Рисунке 4. На каждом окне защищенных помещений установлены шторы. Системы

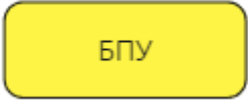


«Соната СА-4Б» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя.



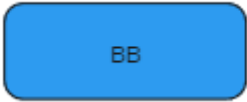

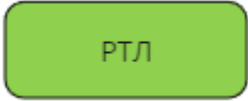

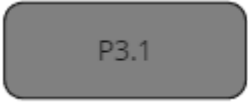
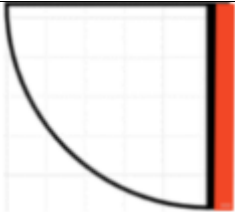
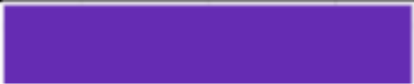
Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 9 приведено описание обозначений устройств.



Рисунок 4 – Размещение инженерно-технических средств защиты информации

Таблица 9 – Описание обозначений устройств

Обозначение	Устройство
	Блок электропитания и управления «Соната-ИП4.3»
	Генератор-акустоизлучатель «Соната СА-4Б»
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)

	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)
	Размыкатель линии «Ethernet» «Соната-ВК4.3»
	Размыкатель телефонной линии «Соната-ВК4.1»
	Размыкатель слаботочной линии «Соната-ВК4.2»
	ПЭМИН «Соната-РЗ.1»
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ» с доводчиком
	Шторы-плиссе BlackOut

5 ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы "Проектирование инженерно-технической системы защиты информации на предприятии" была проведена глубокая аналитика существующей информационной инфраструктуры предприятия, с целью выявления основной деятельности компании и определения защищаемых помещений. На основе результатов анализа была разработана и внедрена инженерно-техническая система защиты информации, нацеленная на обеспечение конфиденциальности, целостности и доступности данных, а также снижение рисков и предотвращение возможных угроз от утечки информации по техническим каналам. Важным этапом в рамках проекта было выявление требований к системе защиты, учет специфики бизнес-процессов и обеспечение соответствия стандартам и регулятивным требованиям в области информационной безопасности. Выбор и внедрение средств защиты, а также их настройка под особенности предприятия, способствовали повышению эффективности системы в целом.

Эта работа позволяет сделать вывод о том, что проектирование и внедрение инженерно-технических систем защиты информации является неотъемлемой частью обеспечения информационной безопасности предприятия. Разработанные в рамках проекта методики и решения могут послужить основой для дальнейшего совершенствования системы защиты и обеспечения безопасности информационных активов предприятия.

6 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. – 151 с. – 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 с.
3. 3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режимдоступа: <https://detsys.ru/> (дата обращения: 28.11.2023).
4. 4. Лаборатория ППШ: Противодействие промышленному шпионажу [Электронный ресурс]. – Режим доступа: <http://www.pps.ru/> (дата обращения 27.11.2023)