

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

«Проектирование инженерно-технической системы защиты информации на
предприятии»

Выполнил:

Чернышова М. В., студент группы N34501


(подпись)

Проверил:

Попов И. Ю., к.т.н., 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	Чернышова Марина Владимировна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Разработать систему инженерно-технической защиты информации на предприятии

Краткие методические указания

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Чернышова Марина Владимировна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) 10.03.01. - Технологии защиты информации


Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Исследование организации и обрабатываемой информации	20.11.2023	20.11.2023	
2	Выявление обоснования для разработки инженерно-технической системы защиты информации	28.11.2023	28.11.2023	
3	Изучение плана предприятия	5.12.2023	5.12.2023	
4	Анализ рынка инженерно-технических средств защиты информации	15.12.2023	19.12.2023	
5	Разработка итоговой инженерно-технической системы защиты информации	17.11.2023	19.11.2023	

Руководитель _____
(Подпись, дата)

Студент  _____
(Подпись, дата)

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

Студент	Чернышова Марина Владимировна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☒ Предложены студентом ☐ Сформулированы при участии студента
☐ Определены руководителем

Цель данной работы – повышение защищённости предприятия с помощью спроектированной инженерно-технической системы защиты информации.

**2. Характер
работы**


- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое

3. Содержание работы

В данной курсовой работе была исследована организации и обрабатываемая на ней информация, приведены обоснования защищаемой информации, изучен план предприятия, проанализирован рынок инженерно-технических средств защиты информации и разработан итоговый план.

4. Выводы

В результате выполнения работы была повышена защищённость предприятия с помощью спроектированной инженерно-технической системы защиты информации.

Руководитель	
	(Подпись, дата)
Студент	
	(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

Введение.....	2
1. Общие сведения о защищаемой организации.....	3
2. Обоснование защищаемой информации.....	5
3. Анализ защищаемого помещения	11
4. Анализ рынка.....	15
4.1 Защита от утечек по оптическим каналам.....	15
4.2 Защита от утечек по акустическим и виброакустическим каналам	15
4.3 Защита от утечки по электрическим и электромагнитным каналам	18
5. Разработка инженерно-технической системы защиты информации.....	21
Заключение	23
Список использованных источников	24

ВВЕДЕНИЕ

Цель работы – повышение защищённости предприятия с помощью спроектированной инженерно-технической системы защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть структуру защищаемого предприятия;
- обосновать защищаемую информацию;
- определить каналы утечки информации и проанализировать рынок;
- предоставить меры активной и пассивной защиты информации.

1. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ

Наименование организации: ООО “SOLUTION”

Область деятельности: Предоставление услуг по разработке систем управления информационной безопасностью (SIEM) государственным структурам.

Основные информационные процессы:

2. публикация рекламных предложений о предоставляемых услугах;
3. предоставление пользователям инструментов для заказа услуги;
4. технологическое сопровождение оказания услуги;
5. предоставление технической поддержки пользователей;
6. удаление данных по завершении сотрудничества;
7. ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией;
8. хранение, обработка, передача, утилизация персональных данных пользователей;
9. хранение данных о конфигурации SIEM-системы клиента;
10. хранение данных о сетевом оборудовании организации;
11. внутреннее взаимодействие сотрудников.

Основные информационные потоки представлены на Рисунке 1.



Рисунок 1 – Основные информационные потоки

Открытые информационные потоки:

- реклама и маркетинг.

Закрытые информационные потоки:

- внутренние коммуникации сотрудников;
- конфиденциальная информация компании (финансовые отчеты, информация о продуктах организации и т. д.).
- Информация ограниченного доступа:
 - персональные данные сотрудников и клиентов;
 - техническая информация (учетные записи, данные локальной сети и т. д.);
- коммерческая тайна;
- государственная тайна (секретно) – заказы, связанные с государственными организациями.

2. ОБОСНОВАНИЕ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Система классифицирована как "Секретно" в связи с обработкой информации, составляющей государственную тайну. Информация приобретает статус государственной тайны, когда поступает от заказчика, представляющего государственные структуры. Таким образом, исходный код разработанного продукта также относится к информации, составляющей государственную тайну.

Для обоснования защищаемой информации обратимся к нормативной базе. Рассмотрим Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Постановление Правительства РФ от 15.04.1995 N 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.", и Постановление Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51 "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам".

Согласно Закону РФ "О государственной тайне" от 21.07.1993 N 5485–1, статье 5:

Государственную тайну составляют:

1) сведения в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства.

Согласно статье 27:

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

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

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

наличие у них сертифицированных средств защиты информации.

Согласно Постановлению Правительства РФ от 15.04.1995 N 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.", пункту 7:

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

соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51 "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам", статье 1:

Пункт 4. Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

Пункт 7. Основными организационно-техническими мероприятиями по защите информации являются:

- лицензирование деятельности предприятий в области защиты информации;
- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

- обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;
- оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Пункт 9. Проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

3. АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

План защищаемого помещения представлен на Рисунке 2.

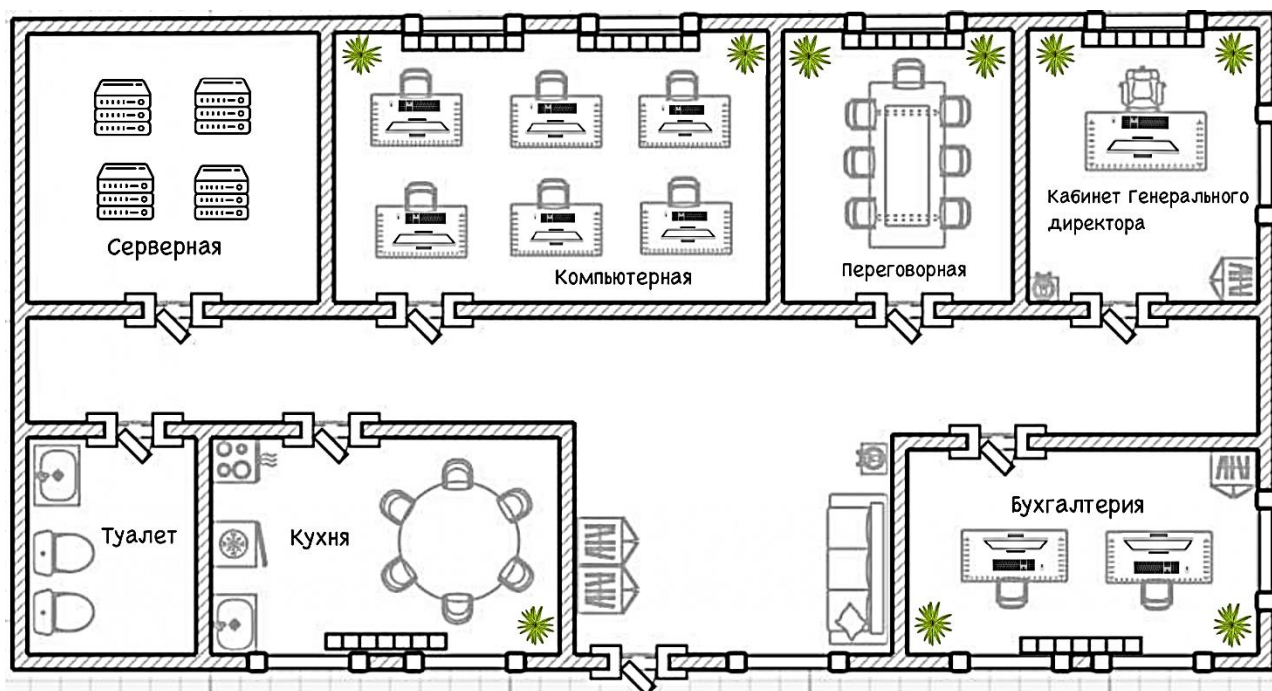
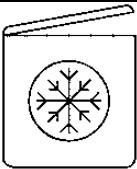
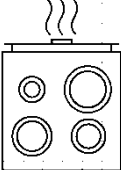
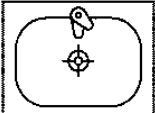
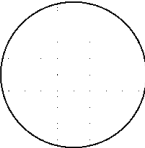

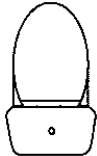
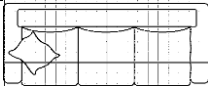

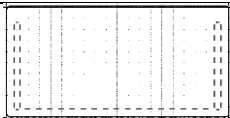
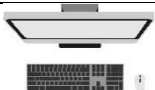

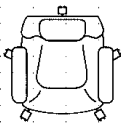
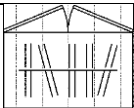





Рисунок 2 – План защищаемого помещения

Условные обозначения представлены в Таблице 1.

Таблица 1 – Условные обозначения

Обозначение	Описание
	Холодильник
	Электрическая плита
	Раковина
	Обеденный стол

	Стул
	Унитаз
	Диван
	Переговорный стол
	Рабочий стол
	Стационарный компьютер
	Сервер
	Кресло руководителя
	Гардеробный шкаф
	Кулер
	Радиатор отопления
	Горшок с цветком

Помещения, требующие защиты, поскольку в них производится обработка сведений, составляющих коммерческую тайну:

- кабинет генерального директора (20 кв.м.);
- переговорная (20 кв.м.);
- серверная (25 кв.м.);
- компьютерная (30 кв.м.);

– бухгалтерия (22 кв.м.).

В кабинете генерального директора находятся 1 рабочий стол, 1 кресло руководителя, 1 стационарный компьютер, 1 гардеробный шкаф, 1 кулер, 2 цветка в горшке, 2 окна, 1 радиатор отопления.

В переговорной находятся 1 переговорный стол, 7 стульев, 2 цветка в горшке, окно, 1 радиатор отопления.

В серверной находятся 4 сервера.

В компьютерной находятся 6 рабочих стола, 6 стульев, 6 стационарных компьютеров, 2 цветка в горшках, 2 окна, 2 радиатора отопления.

В бухгалтерии находятся 2 рабочих стола, 2 стула, 2 стационарных компьютера, 1 гардеробный шкаф, 2 цветка в горшке, 3 окна, 1 радиатор отопления.

На кухне находятся 1 электрическая плита, 1 холодильник, 1 раковина, 1 обеденный стол, 6 стульев, 2 окна, 1 радиатор отопления.

В туалете находятся 2 унитаза и 1 раковина.

В холле находятся 2 гардеробных шкафа, 1 диван, 1 кулер, 1 окно.

Помещение находится на втором этаже здания высотой в пять этажей. Здание расположено на охраняемой территории отдельно от других зданий. Окна находятся вдали от лестниц, используемых для пожарной безопасности и эвакуации. Рядом с окнами отсутствуют дополнительные пристройки, балконы или другие структуры, которые могли бы быть использованы для проникновения посторонних лиц в помещение.

Таким образом, возможные каналы утечки информации и средства защиты, которыми необходимо оснастить помещение для обеспечения инженерно-технической безопасности представлены в Таблице 2.

Таблица 2 – Каналы утечки и средства защиты

Канал утечки	Источники	Пассивная защита	Активная защита
Оптический	Окна, двери	Защитные экраны	Жалюзи или шторы на окнах, доводчики на дверях
Акустический,	Окна, двери,	Сетевые фильтры,	Устройства

акустоэлектрический	проводка	звукоизоляция, обязательное закрытие окон во время совещаний	акустического зашумления
Вибрационный, виброакустический	Радиаторы отопления, трубы, стены, пол, окна, двери	Изолирующие звук и вибрацию материалы стен	Устройства вибрационного зашумления
Электрический, электромагнитный	АРМ, серверное оборудование, розетки	Сетевые фильтры	Устройства электромагнитного зашумления

4. АНАЛИЗ РЫНКА

Проведём анализ рынка инженерно-технических средств защиты информации и выберем решения, соответствующие нашим каналам утечки информации.

4.1 Защита от утечек по оптическим каналам

Для защиты от утечек по оптическому каналу через окна и двери необходимо установить жалюзи или шторы и доводчики соответственно.

Для удобства эксплуатации было выбрано использование рулонной шторы Blackout 60x175 см за 780 руб/шт., а также дверной доводчик Vanger DC-180-SL за 1917 руб/шт.

4.2 Защита от утечек по акустическим и виброакустическим каналам

В качестве пассивной защиты будут использоваться звукоизоляционные усиленные двери за 29 790 руб/шт. Для обеспечения звукоизоляции переговорной комнаты и кабинета генерального директора используются специальные материалы для звукоизоляции стен.

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. Анализ решений, представленных на рынке, отражён в Таблице 3.

Таблица 3 – Анализ средств активной защиты

Устройство	Описание	Характеристики	Стоимость (руб/шт.)
Генераторный блок «ЛГШ-404»	Предназначено для защиты акустической речевой информации от утечки по виброакустическому и	Диапазон частот 175-11200 Гц; Количество подключаемых излучателей на канал до	35 100

	акустическому каналам. Изделие соответствует типу «А» – средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными преобразователями.	20 шт; Мощность, потребляемая от сети не менее 25 ВА	
Устройство подавления диктофонов и микрофонов «Бубен Ультра МАКС»	Предназначен для подавления звукового сигнала при попытке записывающие устройства, специальные технические средства, выносные микрофоны посредством генерации трех типов помех.	Частота приемника/передатчика РПДУ 433 МГц; Количество ультразвуковых излучателей, до 48 шт.	67 200
Акустический подавитель диктофонов «Троян-2»	Для подавления всех существующих диктофонов, в т.ч. в сотовых телефонах, любых радиомикрофонов, предотвращение съема акустической информации со стекол, стен и других инженерных конструкций здания.	Уровень звукового давления 80 дБ; Напряжение сигнала помехи на линейном выходе 0,25 В	24 900
Подавитель диктофонов - «Канонир-К7»	Использует сразу 2 способа защиты от прослушки. Подавление происходит с помощью генерации звуковой речеподобной помехи и ультразвука.	Уровень звукового давления 100 дБ / 95 - 100 дБ; Дальность подавления диктофонов, до 2 - 4 м	37 000
Подавитель диктофонов - «ULTRASONIC-SPYLINE-24-LIGHT»	Виброакустические излучатели мешают проникновению лазерных микрофонов и сбору информации с оконных стекол переговорных залов, тем самым обеспечивая надежную защиту и	Уровень звукового давления 90 дБ; Кол-во излучателей 24; Дальность подавления диктофонов, до 1.5 - 5 м	24 800

	конфиденциальность.		
«SEL SP-157G» - генератор акустических и виброакустических помех системы «SEL-157 ШАГРЕНЬ»	Предназначен для защиты речевой информации в помещениях от её утечки по техническим каналам: акустическому, вибрационному и лазерному путём создания маскирующих акустических помех в смежных воздушных пространствах и маскирующих вибрационных помех в ограждающих конструкциях и инженерно-технических коммуникациях.	Частоты 250, 500, 1000, 2000, 4000 и 8000 Гц; Диапазон регулировки общего интегрального уровня шумового сигнала 30Дб	47 400
Система акустических и виброакустических помех «Буран»	Средство активной акустической и вибрационной защиты акустической речевой информации типа А, соответствует требованиям ФСТЭК России к средствам защиты акустической речевой информации по 2 классу защиты и может устанавливаться в выделенных помещениях.	Диапазон частот 100 – 11 200 Гц Диапазон регулировки общего интегрального уровня шумового сигнала 30Дб; Максимальное число изделий, объединяемое в одну группу для их группового подключения к сети электропитания 20 шт.	67 500
«Соната ИП-4.1»	Составная часть системы виброакустической защиты для выделенных помещений и защиты от прослушивания кабинетов первых лиц и переговорных комнат	Нагрузочная способность не менее 1500 мА Мощность, потребляемая от сети не более 40 Вт	26 400
«SEL-310 КОМАР» - портативный ультразвуковой подавитель звукозаписывающих устройств	Предназначен для полного подавления полезного звукового сигнала при попытке записи.	Диапазон частот УЗ помехи 24 - 26 кГц; Кол-во излучателей 10 шт; Дальность подавления диктофонов, до 4 м	58 000

По итогам анализа была выбрана система «ЛГШ-404» в качестве выбранного генераторного блока. Конструкция данного изделия обеспечивает защиту органов регулировки выходного шумового сигнала от

несанкционированных изменений и предотвращает несанкционированный доступ к ним. Кроме того, был выбран подавитель микрофонов и диктофонов «Бубен Ультра МАКС». Он создает три типа помех: ультразвуковые помехи, оказывающие воздействие на мембрану микрофона; сложные акустические помехи, воздействующие на автоматическую регулировку записывающего устройства, усиливающие эффект ультразвуковых помех; помехи, имитирующие речь с изменением характеристик со временем, что затрудняет их выделение из основного звукового сигнала.

4.3 Защита от утечки по электрическим и электромагнитным каналам

Пассивные меры безопасности включают установку фильтров на электрические сети, чтобы минимизировать сигнал от источника информативного сигнала.

Активные меры безопасности основаны на создании в сети фонового шума, который маскирует изменения, вызванные воздействием звуковых волн или функционированием электротехники, чтобы затруднить техническую разведку или нарушить нормальную работу устройств для скрытого сбора информации, и представлены в Таблице 4.

Таблица 4 – Анализ средств активной защиты

Устройство	Описание	Характеристики	Стоимость (руб./шт.)
Генератор шума «ЛГШ-503»	Предназначено для защиты информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих	Диапазон частот 10 кГц - 1800 МГц; Уровень шума от -26дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц); Мощность 45 Вт Наработка на отказ 12000 часов	44 200

	шумоподобных помех.		
Генератор шума «ГАММА ГШ-18»	Предназначен для маскировки ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей и комплексов на объектах вычислительной техники второй, третьей и четвертой категорий, путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) и наведения шумового сигнала на токопроводящие линии и инженерно-технические коммуникации, включая цепи электропитания и заземления, в широком диапазоне частот.	Диапазон частот от 0,01 до 1800 МГц; Уровень шума уровень сигнала на нагрузке 50 Ом во всем диапазоне частот не менее 50 дБ/мкВ, диапазон регулировки выходного сигнала от 0 до 20 дБ; Мощность 50 дБ/мкВ; Наработка на отказ 20000 ч.	29 400
Генератор шума «ГНОМ-3М»	Предназначен для активной защиты информации, обрабатываемой на электронно-вычислительной технике.	Диапазон частот 0,15 до 1800 МГц; Уровень шума 25 - 75 дБ/мкВ; Мощность 40 Вт	57 200
Фильтр сетевой помехоподавляющий «ФСП-1Ф-7А»	Предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации по цепям электропитания с напряжением 220 В с током нагрузки до 7 А.	Диапазон частот 0,15-1000 МГц; Вносимое затухание по напряжению в каждом проводе двухпроводной сетине не менее 60 дБ; Допустимый ток нагрузки 7 А	54 920
Фильтр сетевой помехоподавляющий «ФПБД»	Предназначен для защиты информации на различных устройствах типа вычислительной техники и прочих радиоэлектронных устройствах, где	Ток 15 А; Частотный диапазон от 0,01 до 1000 МГц; Затухание 30 до 60 дБ	19 875

	возможна утечка посредством наводок по электрическим цепям.		
Фильтр сетевой помехоподавляющий «ФСШК-2»	Предназначен для защиты информации на различных устройствах типа вычислительной техники и прочих радиоэлектронных устройствах, где возможна утечка посредством наводок по электрическим цепям.	Ток 6 А; Частотный диапазон от 0,01 до 1000 МГц; Затухание 40 до 70Дб	19 125

По результатам анализа был выбран генератор шума «ГАММА ГШ-18». Это устройство обеспечивает плавное регулирование уровня выходного сигнала, характеризуется широким диапазоном функциональности и представляет собой экономически эффективное решение. Кроме того, отлично подходит для маскировки ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей. Для реализации пассивной защиты был выбран фильтр сетевой помехоподавляющий «ФПБД», способный эффективно подавлять помехи в сети электропитания, что способствует снижению риска утечки информации.

Поскольку в предыдущем пункте в качестве генераторного блока была выбрана система «ЛГШ-404», то выберем, входящие в состав данной системы размыкатель слаботочных линий – «ЛУР 2» за 5 590 руб/шт и размыкатель линий Ethernet – «ЛУР 8» за 5 590 руб/шт.

5. РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

На основании анализа предшествующих разделов был разработан план помещений для предприятия "SOLUTION" с учётом инженерно-технических мер, направленных на обеспечение защиты информации от возможных утечек (Рисунок 3).

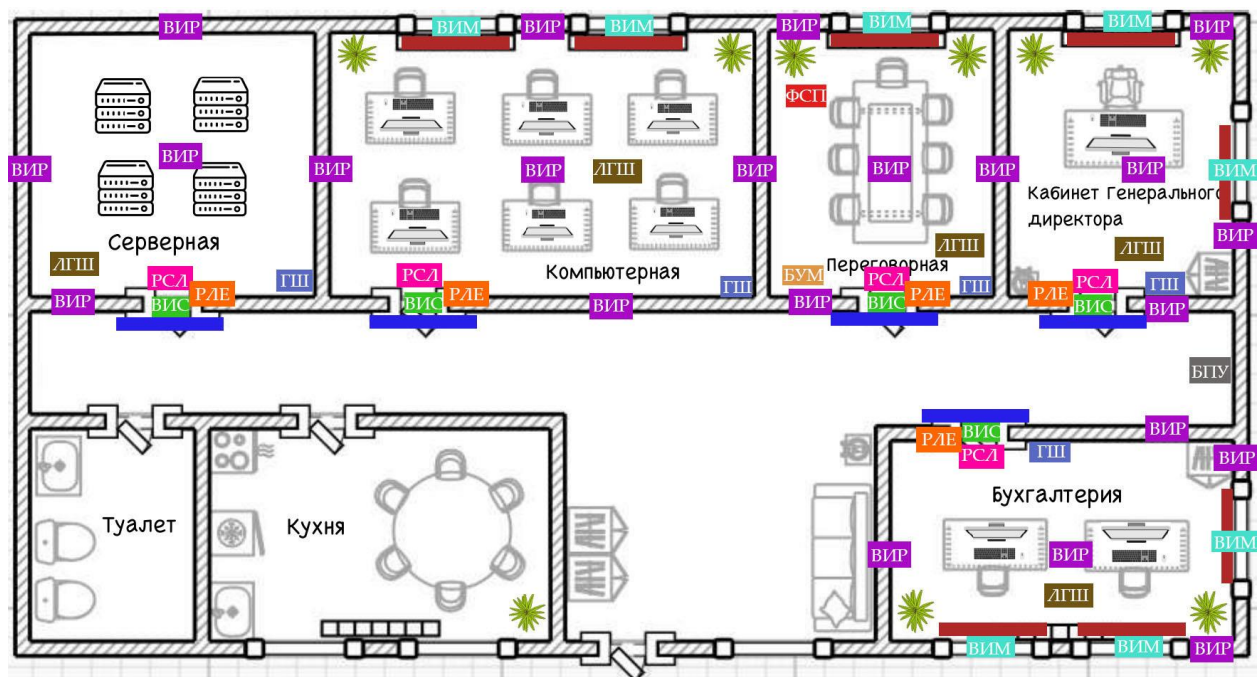










Рисунок 3 – План помещения с инженерно-техническими средствами защиты информации

В Таблице 5 представлены выбранные инженерно-технические средства защиты информации и их условные обозначения.

Таблица 5 – Обозначения средств защиты

Средство защиты	Обозначение
Рулонная штора Blackout	
Звукоизоляционная усиленная дверь	
Блок питания и управления «Гамма-01 БПУ»	
Вибрационный излучатель «Серп» (двери)	

Вибрационный излучатель «Серп-Р» (стены, пол)	
Вибрационный излучатель «Молот» (окна)	
Фильтр сетевой помехоподавляющий «ФПБД»	
Генератор шума «Гамма ГШ-18»	
Подавитель микрофонов и диктофонов «Бубен Ультра МАКС»	
Генераторный блок «ЛГШ-404»	
Размыкатель слаботочных линий «ЛУР 2»	
Размыкатель линий Ethernet «ЛУР 8»	

ЗАКЛЮЧЕНИЕ

В ходе курсовой работы были проанализированы существующие технические каналы утечки информации, возможные технические каналы утечки информации для защищаемого помещения организации ООО «SOLUTION», которая работает с государственной тайной уровня «секретно». По результатам анализа помещения был проанализирован рынок существующих средств для противодействия рассматриваемым каналам утечки информации и выбраны необходимые инженерно-технические средства защиты информации.

Таким образом, была предложена защита от утечек информации по оптическому, акустическому, виброакустическому, электрическому, электромагнитному каналам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон Российской Федерации “О государственной тайне” от 21.07.1993 N 5485-1 (дата обращения: 15.12.2023)
2. Постановление Правительства РФ “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 15.04.1995 N 333 (дата обращения: 15.12.2023)
3. Постановление Совета Министров – Правительства РФ “О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам” от 15.09.1993 N 912-15 (дата обращения: 15.12.2023)
4. Кармановский Н.С., Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие. – Текст: электронный. – 2013. – URL: https://e.lanbook.com/book/43579__ (дата обращения: 15.12.2023)