

**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 системы защиты от утечки информации
по различным каналам

Выполнил:

студент группы N34501
Акжигитов Р.А.



Проверил:

к.т.н., доцент ФБИТ
Попов И.Ю.

Отметка о выполнении:

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Акжигитов Руслан Андреевич (фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении
Задание	Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации»;
2. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины;
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
4. Анализ защищаемых помещений
5. Анализ рынка технических средств
6. Описание расстановки технических средств
7. Заключение
8. Список литературы

Рекомендуемая литература

1. 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

Руководитель

(Подпись, дата)

Студент

Акжигитов


(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент	Акжигитов Руслан Андреевич
	(фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023	01.10.2023	
2	Анализ источников	01.11.2023	01.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	01.12.2023	01.12.2023	
4	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

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

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Акжигитов Руслан Андреевич (фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА
(РАБОТЫ)**

Цель и задачи работы	Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
Характер работы	Конструирование
Содержание работы	1. Введение. 2. Анализ технических каналов утечки информации. 3. Руководящие документы 4. Анализ защищаемых помещений 5. Анализ рынка технических средств 6. Описание расстановки технических средств 7. Заключение 8. Список литературы
Выводы	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
Цель работы.....	6
Задачи.....	6
ОСНОВНАЯ ЧАСТЬ	7
1 Анализ защищаемой организации	7
1.1 Общее описание	7
1.2 Информационные потоки	7
1.3 Защищаемое помещение	8
2. Анализ нормативно-правовой базы.....	11
3. Анализ рынка средств защиты информации.....	12
4. Разработка инженерно-технической системы защиты информации	16
ЗАКЛЮЧЕНИЕ	17
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	18

ВВЕДЕНИЕ

Цель работы

Повышение защищенности рассматриваемого помещения.

Задачи

- Анализ защищаемого помещения
- Оценка каналов утечки информации
- Выбор мер пассивной и активной защиты информации

ОСНОВНАЯ ЧАСТЬ

1 Анализ защищаемой организации

1.1 Общее описание

Наименование организации: ООО “Натлан”

Область деятельности: Комплекс услуг по обеспечению информационной безопасности.

Организация ориентирована на B2B. Предоставляет услуги в сферах тестирование на проникновение, консалтинг, защита персональных данных, аудит, расследования, техническая защита информации

Организация планирует расширяться в сторону B2G, а именно обследование и категорирование объектов КИИ, проектирование и внедрение СЗ. В частности, связанных со сведениями, составляющими государственную тайну уровня “секретно”. Как следствие, необходимо оборудовать арендованное офисное помещение техническими средствами защиты информации.

1.2 Информационные потоки

Так как компания занимается предоставлением услуг информационной безопасности часть разработчиков, и ИБ-специалистов могут пересекаться в зависимости от проекта. Разработка ПО производится небольшими группами по 4–6 человек, всегда есть сотрудники отдела ИБ, которые не заняты проектами, а обслуживают организацию.

Отдел продаж связывает разработчиков и заказчика. Группа HR занимается подбором, удержанием и увольнением персонала. Бухгалтерия связывает компанию с внешними организациями.

Большая часть отделов компании не имеет доступ к гос. тайне. Потоки, в которых может проходить информация, содержащая гос. тайну на схеме обозначены красным. (рисунок 1)

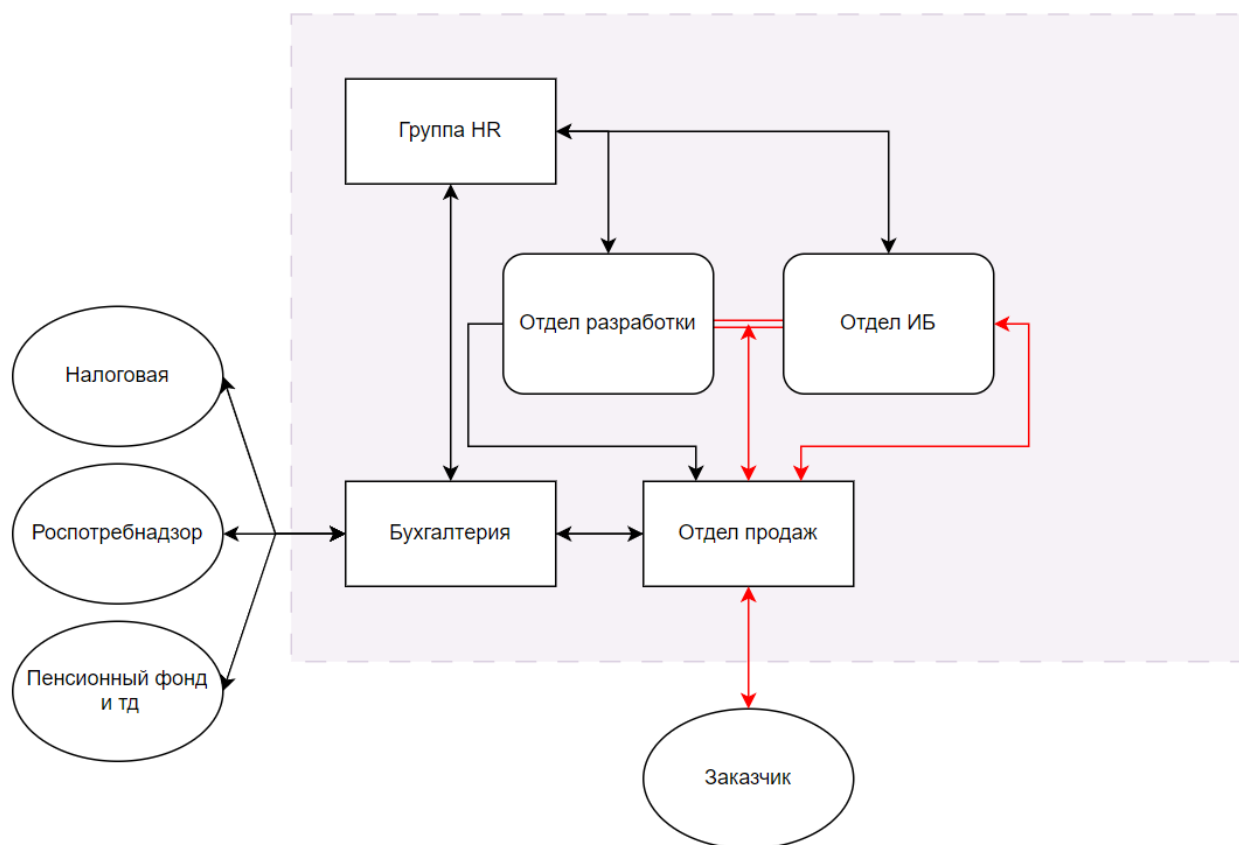


Рисунок 1 - Схема информационных потоков «Натлан»

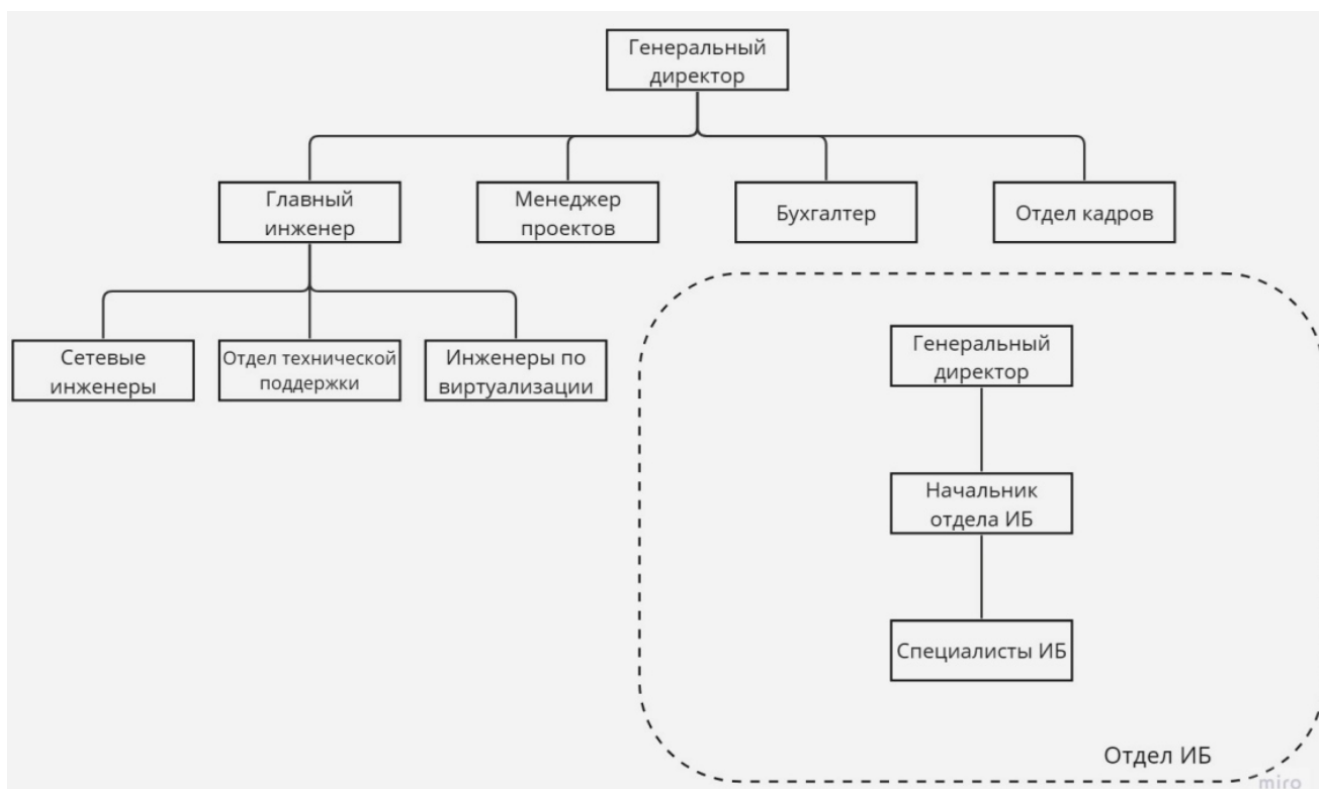


Рисунок 2 – Структура предприятия «Натлан»

1.3 Защищаемое помещение

Офис «Натлан» будет находится на 39 этаже 40-этажного бизнес-центра.

Доступы к помещениям здания ограничен системой контроля и управления доступом.

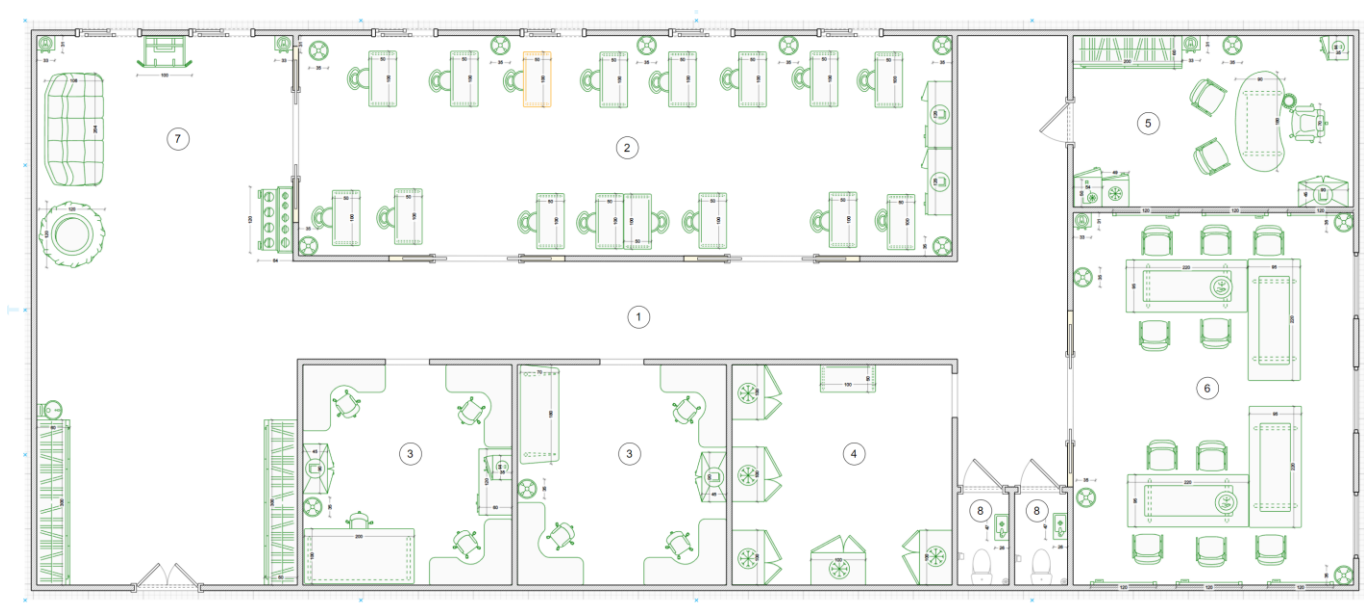


Рисунок 3 - План помещения



Рисунок 4 – Обозначение облементов

Легенда:

— Коридор – подразумевается использование звукоизолированных дверей в тех помещениях, где могут проходить переговоры, содержащие гос. тайну. Поэтому не будет проблем с утечкой акустической информации

- Оpen-спасе офис – офис для основной массы сотрудников в нем не ведутся разработки гос. заказов, не проходят переговоры, содержащие гос. тайну.
- Комната закрытой разработки 2шт. – основные помещения по работе с гос. тайной. Должны быть защищены наилучшим образом. Так как переговорная отведена под нужды организации и не подразумевает обсуждения гос. тайны эти комнаты будут местом где команда сможет обсудить гос. проект
- Переговорная – служит для обсуждения проектов не содержащих гос. тайну
- Офис директора – могут проводиться переговоры или обрабатываться информация, содержащая гос. тайну. Заказчик (государство) сможет обсудить детали проекта именно в кабинете директора
- Пространство отдыха – небольшое пространство рядом с open-спасе офисом. Те кто выполняет гос. заказ не будут отдыхать, они будут работать до потери пульса.
- Серверная - оборудована специальной системой вентиляции и охлаждения, системой бесперебойного питания.
- Санузлы 2 шт.

Таблица 1 – площадь помещений

Номер	Название	Площадь, м ²
1	Коридор	37,60 м2
2	Open-спасе офис	41,51 м2
3	Комната закрытой разработки x2	15,21 м2 x 2
4	Серверная	16 м2
5	Офис директора	15,87 м2
6	Переговорная	34,47 м2
7	Пространство отдыха	46,88 м2
8	Санузел x2	1,58 + 1,62 м2

Таблица 2 - Возможные каналы утечки информации

Номер помещения	Каналы утечки						
	Беспроводная и сотовая	Акустический канал	Виброакустический канал	Сеть питания 220/380	ПЭМИН	Слаботочные линии	Оптический канал

	СВЯЗЬ			В			
1	*	*	*		*	*	*
3	*	*	*		*	*	*
4				*	*		
5	*	*	*		*	*	*
6	*	*	*		*	*	*
7	*	*	*		*	*	*

2. Анализ нормативно-правовой базы

При разработке комплекса 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 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
- ГОСТ Р ИСО/МЭК 27001-2021 “Системы менеджмента

информационной безопасности. Требования”; — ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”;

— ГОСТ Р ИСО/МЭК 27033-2011 “Безопасность сетей”.

Для получения лицензии на работу с государственной тайной степени “секретно” необходимо выполнить следующие требования:

- 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; —
- 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.

3. Анализ рынка средств защиты информации

Ниже приведено сравнение рынка и инженерно-технической защите информации по следующим категориям:

- **Блокираторы беспроводная и сотовая связь** - предназначены для пресечения нелегального функционирования устройств, которые могут несанкционированно получать информацию в сетях сотовой связи, а также в стандартах Bluetooth и WiFi. Принцип их работы основан на генерации шумовых помех в соответствующих частотных диапазонах, что обеспечивает активную защиту от несанкционированного доступа.
- **Акустическое зашумление** - разработано для предотвращения эффективного использования специальных устройств несанкционированного съема информации, которые могут использовать воздушную среду помещения в качестве канала утечки. Такие устройства включают в себя микрофоны и диктофоны. Этот метод представляет собой активную защиту от потенциальных угроз конфиденциальности
- **Виброакустическое зашумление** - предназначена для противодействия специальным средствам, направленным на несанкционированный сбор информации и использующим ограждающие конструкции помещения в качестве канала утечки. К таким средствам можно отнести: стетоскопы, радиомикрофоны, лазерные и микроволновые системы съема информации
- **Защита сети питания 220/380В** – защиту разделяют на пассивную и активную. Пассивные методы защиты сети переменного тока (220 В) от несанкционированного съема информации включают использование сетевых помехоподавляющих фильтров. Эти фильтры блокируют передачу информативных сигналов, генерируемых при работе оргтехники, и, при правильной установке, защищают устройства от внешних помех. Важно учесть, что для эффективной работы помехоподавляющих фильтров требуется надежное заземление. Активные методы защиты сети переменного тока (220 В) включают использование генераторов шумовых сигналов. Эти сигналы превосходят по уровню сигналы устройств съема информации или информативные сигналы, обеспечивая эффективную защиту от несанкционированного доступа.

- **ПЭМИН** - побочные электромагнитные излучения и наводки могут быть перехвачены с помощью специальной аппаратуры. Генераторы радиопомех предназначены для работы в составе систем активной защиты информации (САЗ), обеспечивая защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта. Это является активной защитой.
- **Защита слаботочных линий** – **существует** комплекс мер и технических средств, направленных на обеспечение безопасности, надежности и конфиденциальности передаваемой информации по слаботочным (низковольтным) линиям и средствам связи. К таким линиям и средствам обычно относятся телефонные, компьютерные и другие сети передачи данных.
- **Защита визуально-оптического канал** – зашторить окна обычно хватает для закрытия большинства проблем связанных с оптическим каналом

Таблица 3 - Блокираторы беспроводной и сотовой связи

Название устройства	Производитель	Описание	Цена
ЛГШ-725	Лаборатория ППШ	Блокиратор сотовой связи стандартов: <ul style="list-style-type: none"> - IMT-MC-450 - GSM900 - DSC/GSM1800 - LTE 2600 - Bluetooth - WiFi 2.4 / 5 ГГц 	247 000 руб.
ЛГШ-723	Лаборатория ППШ	Блокиратор работы устройств, работающих в стандартах: <ul style="list-style-type: none"> - Bluetooth - WiFi 2.4 / 5 ГГц 	117 000 руб.
ЛГШ-701	Лаборатория ППШ	Блокиратор стандарта: <ul style="list-style-type: none"> - IMT-MC-450 - GSM900 - DSC/GSM1800 	97 500 руб.

Таблица 4 - Акустическое зашумление и виброакустическое

Название устройства	Производитель	Описание	Цена
ЛГШ-404	Лаборатория ППШ	Изделие соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными преобразователями	35 100 руб.
ЛАГ-105	Лаборатория ППШ	Особенности: <ul style="list-style-type: none"> - Вместимость до 10 телефонов - Возможно нанесение логотипа 	67 600 руб.

Название устройства	Производитель	Описание	Цена
		Вашей компании на внешнюю сторону корпуса	
ЛВП-2а	Лаборатория ППШ	Акустический излучатель предназначен для возбуждения маскирующих акустических помех в различных закрытых пространствах	5 200 руб.

Таблица 5 - Защита сети 220/380В

Название устройства	Производитель	Описание	Цена
ЛФС-40-1Ф	Лаборатория ППШ	ЛФС-40-1Ф соответствует типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.	70 200 руб.
ЛФС-10-1Ф	Лаборатория ППШ	Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну,	47 060 руб.
ЛФС-200-3Ф	Лаборатория ППШ	Изделие включается в трехфазную четырехпроводную сеть напряжением (380+10%) В частоты 50 Гц без соблюдения полярности. Режим работы Изделия автоматический, круглосуточный.	377 000 руб.

Таблица 6 - Пространственное зашумление (защита от ПЭМИН)

Название устройства	Производитель	Описание	Цена
ЛГШ-504	Лаборатория ППШ	Генератора шума «ЛГШ-504НЧ» - генератора низкочастотного сигнала (диапазон частот от 0,009 до 30 МГц, может использоваться с внешними рамочными антеннами)	156 000 руб.
ЛГШ-516СТАФ	Лаборатория ППШ	Изделие «ЛГШ-516СТАФ» соответствует 2 классу защиты. Изделие «ЛГШ-516СТАФ» соответствует требованиям документа	51 000 руб.

Название устройства	Производитель	Описание	Цена
ЛГШ-501	Лаборатория ППШ	Изделие «ЛГШ-501» является: - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»)	29 900 руб.

Таблица 7 - Защита слаботочных линий и линий связи

Название устройства	Производитель	Описание	Цена
Гранит-8	Лаборатория ППШ	Назначение фильтра пропускать сигналы в речевом диапазоне частот при нормальном режиме работы телефонной линии и ослаблять высокочастотные сигналы, которые могут подаваться в линию при высокочастотном навязывании.	4 160 руб.
ЛУР 2 (в составе ЛГШ-404)	Лаборатория ППШ	Размыкатель слаботочных линий питания	35 100 руб.
ЛУР 4 (в составе ЛГШ-404)	Лаборатория ППШ	Размыкатель слаботочных линий Телефон	35 100 руб.

Подводя итог можно выделить следующие СЗИ
Таблица 8 – выбранные решения

Категория	Название устройства	Производитель	Цена
Блокираторы беспроводной и сотовой связи	Лаборатория ППШ	ЛГШ-725	247 000 руб.
Виброакустическое и акустическое зашумление	Лаборатория ППШ	ЛГШ-404	35 100 руб.
Защита сети 220/380В	Лаборатория ППШ	ЛФС-40-1Ф	70 200 руб.
Пространственное зашумление	Лаборатория ППШ	ЛГШ-504	156 000 руб.

Категория	Название устройства	Производитель	Цена
Защита слаботочных линий и линий связи	Лаборатория ПППШ	ЛУР 2 (в составе ЛГШ-404)	35 100 руб.
Визуально-оптическая защита	Лаборатория ПППШ	ЛИСТ-1 (в составе ЛГШ-404)	35 100 руб.

4. Разработка инженерно-технической системы защиты информации

На основе анализа плана помещения защищаемой организации, перечня руководящих документов и рынка средств защиты информации была разработана следующая инженерно-техническая система защиты информации для предприятия организации «Натлан».



Рисунок 3 - План помещения с техническими средствами защиты информации

Легенда:

- АЗ - Система постановки акустических помех;
- ББС - Блокиратор беспроводной связи;
- ВАЗ - Система постановки виброакустических помех;
- ГШ - Генератор шума ПЭМИ;
- Р - Размыкатель Ethernet;
- РС - Размыкатель слаботочных сетей;
- СГШ - Сетевой генератор шума;
- СФ - Сетевой помехоподавляющий фильтр;
- ШТ – Рулонная штора

ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта, была разработана инженерно-техническая система защиты информации для организации «Натлан» предоставляющей услуги по обеспечению информационной безопасности в B2B и B2G сегментах. В ходе работы были проанализированы рынок инженерно-технических средств защиты информации, а также нормативная база в областях информационной безопасности, государственной тайны и государственной тайны степени «секретно»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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