

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

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

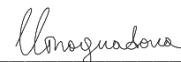
ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Проектирование инженерно-технической
защиты информации на предприятии»

Выполнил:

студент группы N34511

Виноградова Екатерина Сергеевна



(подпись)

Проверил:

доцент ФБИТ, к.т.н.

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Виноградова Е.С. (Фамилия И.О.)
Факультет	факультет безопасности информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Информационная безопасность
Руководитель	Попов И.Ю. (Фамилия И.О.)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 109
Задание	Разработать проект инженерно-технической системы защиты информации для предприятия.

Краткие методические указания

Содержание пояснительной записки

Работа включает в себя разработку проекта ИТСЗИ для предприятия

Курсовая работа включает разделы:

Введение;

1. Анализ помещения предприятия;
2. Оценка каналов утечки информации;
3. Выбор и размещение мер пассивной и активной защиты информации;

Заключение

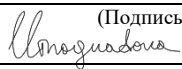
Рекомендуемая литература

ГОСТ Р ИСО/МЭК 27004–2021. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

Руководитель

Студент

(Подпись, дата)



18.12.2023 г.

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Виноградова Е.С.
(Фамилия И.О.)

Факультет факультет безопасности информационных технологий

Группа N34511

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов И.Ю.
(Фамилия И.О.)

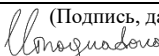
Должность, ученое звание, степень Доцент ФБИТ, кандидат технических наук

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 109

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Заполнение задания на курсовую работу	15.10.2023	15.10.2023	
2.	Анализ информации	25.10.2023	10.12.2023	
3.	Написание курсовой работы	01.11.2023	07.12.2023	
4.	Защита курсовой работы	15.12.2023	19.12.2023	

Руководитель _____

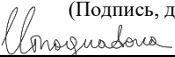
Студент  (Подпись, дата) 15.12.2023 г.
(Подпись, дата)

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

Студент	Виноградова Е.С. (Фамилия И.О.)
Факультет	факультет безопасности информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 Информационная безопасность
Руководитель	Попов И.Ю. (Фамилия И.О.)
Должность, ученое звание, степень	Доцент ФБИТ, кандидат технических наук
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 109

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	Разработка проекта по обеспечению защиты информации в предприятии с помощью инженерно-технических средств
2. Характер работы	Отчетная курсовая работа
3. Содержание работы	Курсовая работа включает разделы: Введение; 1. Анализ помещения предприятия 2. Оценка каналов утечки информации; 3. Выбор и размещение мер пассивной и активной защиты информации; Заключение.
4. Выводы	

Руководитель	 (Подпись, дата)
Студент	 07.12.2023 г. (Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1 АНАЛИЗ ПОМЕЩЕНИЯ ПРЕДПРИЯТИЯ.....	7
1.1 Описание предприятия	7
1.2 Обзор помещения	8
2 ОЦЕНКА КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	11
3 ВЫБОР И РАЗМЕЩЕНИЕ МЕР ПАССИВНОЙ И АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ	12
3.1 Выбор и установка средств защиты	12
ЗАКЛЮЧЕНИЕ.....	19
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	20

ВВЕДЕНИЕ

Цель работы – разработка проекта обеспечения предприятия инженерно-техническими средствами защиты информации в целях повышения защиты информационной системы от утечек данных.

Задачи, выполняемые в работе:

- Анализ помещения предприятия;
- Оценка каналов утечки информации;
- Выбор и размещение мер пассивной и активной защиты информации.

При разработке проекта были учтены следующие юридические документы:

1. Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;
2. Постановление Правительства РФ от 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
3. Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;
4. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ;
5. ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”.

1 АНАЛИЗ ПОМЕЩЕНИЯ ПРЕДПРИЯТИЯ

1.1 Описание предприятия

Организация, для которой разработан проект по обеспечению инженерно-технических средств информации – НОУ «Кронверкский Барсик».

Данное учреждение относится к частным негосударственным структурам. Необходимо обеспечить защиту коммерческой тайны, персональных данных. Организация предоставляет услуги по обучению детей дошкольного возраста. Для бизнеса было принято решение об оборудовании помещения техническими средствами защиты информации.

К информационным потокам предприятия относятся связь с клиентами, хранение персональных данных клиентов (ИТ отдел), финансовые транзакции (бухгалтерия взаимодействует с налоговой и банком).

Далее на рисунке 1 схематично показана организационная структура «Кронверкского Барсика».

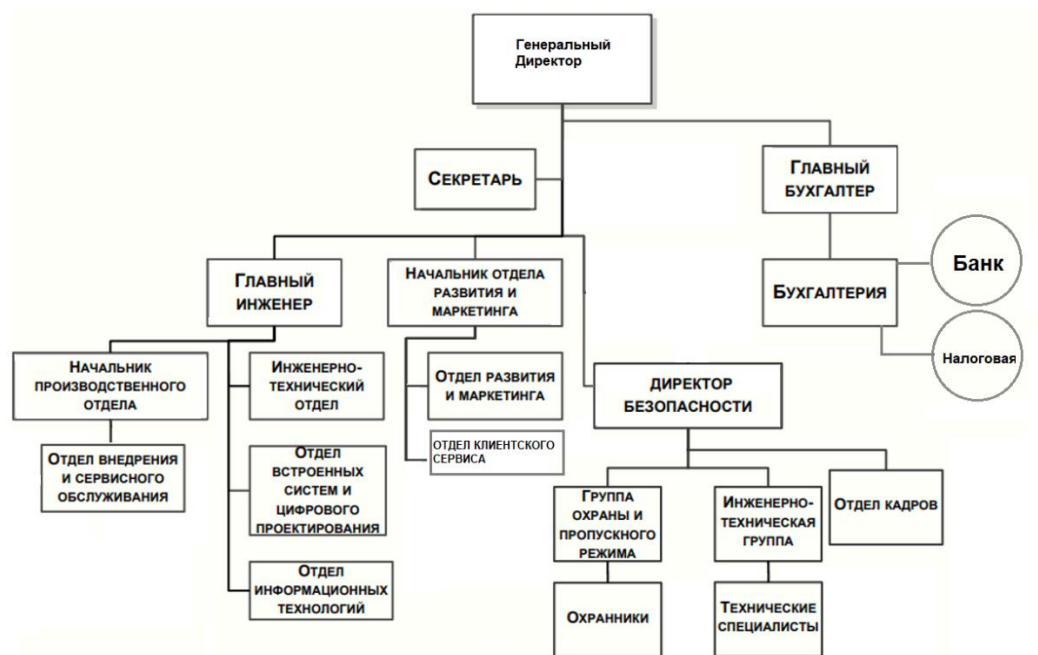


Рисунок 1 – Организационная структура предприятия

Далее на рисунке 2 представлены информационные потоки организации.

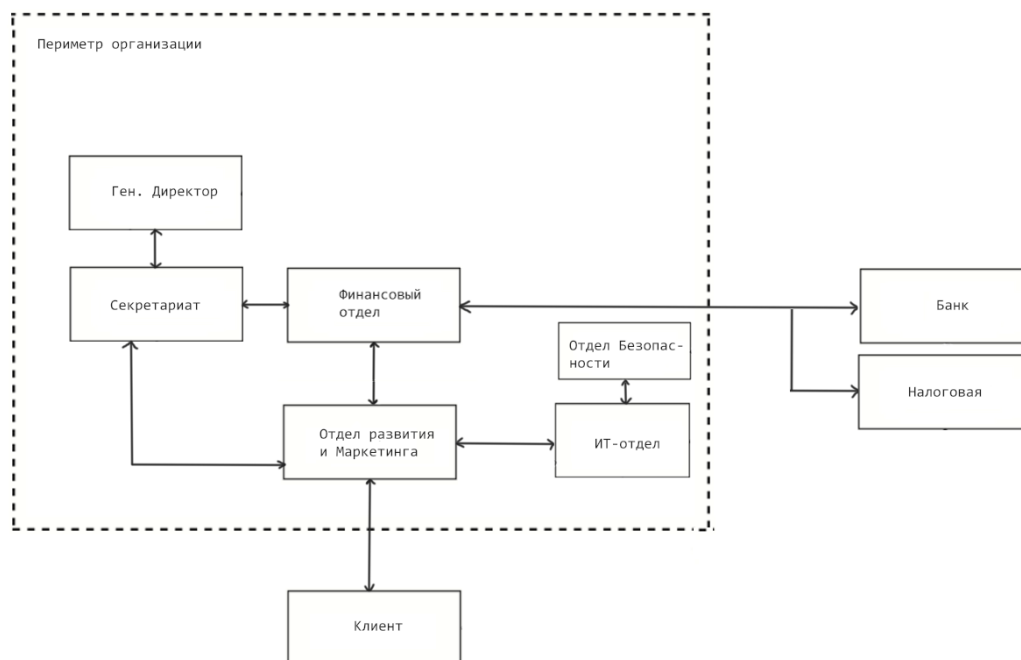


Рисунок 2 – Информационные потоки организации

1.2 Обзор помещения

Помещение организации расположено на первом этаже одноэтажного здания. Окна имеются на северной – кабинет гендиректора, а также восточной частях – отдел технического оснащения и ИТ. Окна также имеются на южной части, где проходят занятия. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Доступы к помещениям здания находится под контролем СКУДа. Допуск в общие помещения имеют клиенты и весь обслуживающий персонал, сотрудники технического отдела. Доступ к кабинету директора имеет только директор. Доступ к бухгалтерии имеет директор и бухгалтерия. К приемной имеют доступ все сотрудники организации. К ИТ-отделу имеют доступ сотрудники технического отдела и работники профессиональной уборки.

Помещение состоит из:

1. Внутреннего коридора;
2. Кабинета директора;
3. Конференц-зала;
4. 9 классов;
5. Уборной;
6. Сантехнического складского помещения;
7. Складского помещения;

8. Актового зала;
9. Кабинета ИТ-отдела;
10. Серверной;
11. Бухгалтерии.

Далее на рисунке 3 представлен план здания «Кронверкского Барсика».

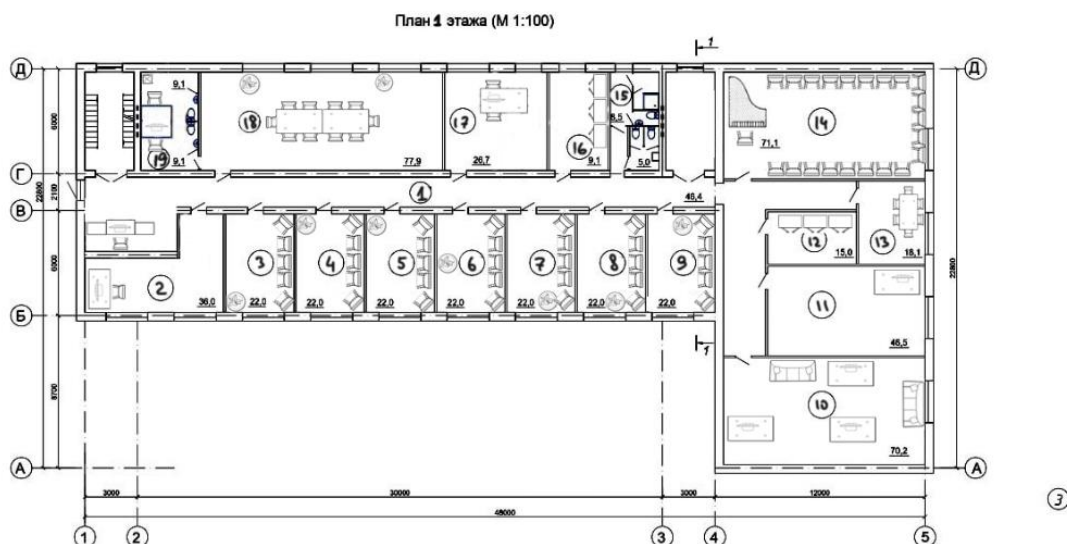


Рисунок 3 – План помещения

Далее на рисунке 4 представлены условные обозначения, используемые на плане защищаемого помещения.



Рисунок 4 – Условные обозначения

Далее в таблице 1 представлен перечень комнат в организации.

Таблица 1 – Перечень комнат

№	Комната, м ²
1	Коридор, 46,4 м ²
2	Коморка охранника 36 м ²
3-9	Классы, 22 м ²
10	Отдел ИТ, 70,2 м ²
11	Серверная, 46,5 м ²

12	Складское помещение, 15 м ²
13	Обеденная, 18,1 м ²
14	Актальный зал, 71,1 м ²
15	Туалет, 13,5 м ²
16	Подсобка сантехническая, 9,1 м ²
17	Бухгалтерия, 26,7 м ²
18	Конференц-зал, 77,9 м ²
19	Кабинет директора, 9,1 м ²

Суммарно в помещении 8 компьютеров, объединенных сетью Интернет.

2 ОЦЕНКА КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Возможные каналы утечки защищаемой информации классифицированы по способу перехвата.

1. Оптический канал

К данному типу перехватов относятся подглядывание с улицы, нарушение конфиденциальности со стороны улицы.

2. Акустический канал

Помещение находится на первом этаже. К данному типу перехватов относится подслушивание, которое может быть осуществлено со стороны окон с помощью направленного микрофона и лазера.

В каждом классе имеются радиаторы отопления. Возможна прослушка с помощью стетоскопов.

3. Электромагнитный канал

Каждая комната оснащена розетками. Возможна прослушка информации с помощью системы электропитания. Имеется проводной канал связи ethernet-кабель, по которому может быть осуществлен съем и навязывание информации.

Работа с конфиденциальной информацией ведется с использованием компьютера генерального директора, а также на компьютерах ИТ-отдела, бухгалтерии.

4. Закладные устройства

Закладное устройство может быть размещено во многих местах клиентского доступа – цветочные горшки, шкафчики, мусорная корзина.

3 ВЫБОР И РАЗМЕЩЕНИЕ МЕР ПАССИВНОЙ И АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Выбор и установка средств защиты

Оптический канал утечки информации

В качестве защиты окон от визуальных утечек подойдут шторы с плотностью ткани от 250 г/м². Для одного окна примерная стоимость выходит 3000 рублей. Установка не требует специализированных навыков, поэтому делегируется на персонал организации. Необходимо зашторить конференц-зал, бухгалтерию и ИТ-отдел - итого 6 окон.

Итоговая сумма: 18000 рублей.

В качестве защиты от утечек через двери необходимо поставить доводчики на важные помещения – кабинет директора, бухгалтерию, ИТ-отдел, итого 4 двери. Оптимальной будет установка доводчика дверного Nora-M 101 до 20 кг стоимостью с НДС 565.5 Р.

Итоговая сумма: 2262 рубля.

Пассивная звукоизоляция

Уместна и необходима в двух кабинетах – директора и бухгалтерии. Так как соседей сверху и снизу нет, необходимо изолировать только стены. Ориентировочная высота потолка – 3 метра, суммарная ширина покрытия – 10 метров. Цена за м² – 4000р. Необходимо полностью изолировать кабинет директора обшивкой. Для бухгалтерии будет достаточно звукоизолирующей двери, такое же решение применимо к кабинету директора, каждая стоит 50000 рублей.

Итоговая сумма: 220 тысяч рублей.

Излучатели виброакустических помех

В таблице 2 приведено сравнение нескольких вариантов установки излучателей виброакустических помех.

Таблица 2 – Излучатели виброакустических помех

Модель	Функционал	Стоимость, руб.
ЛГШ-404	Визуальная система индикации нормального режима работы Визуально-звуковая система индикации аварийного режима (отказа) Счетчик учета времени работы в режиме формирования маскирующих помех (ЖК-дисплей)	35 100

	<p>Контроль и защита органов регулировки уровня выходного шумового сигнала</p> <p>Проводное дистанционное управление и контроль (через программно-аппаратный комплекс «Паутина»)</p>	
ЛГШ-402	<p>Электронные или акустические стетоскопы для прослушивания через потолки, полы и стены. Оснащено визуальной системой индикации нормального режима работы.</p> <p>Проводные или радиомикрофоны, установленные на ограждающие конструкции или водопроводные и отопительные трубопроводы;</p> <p>Лазерные или микроволновые системы съема информации через оконные проемы помещений.</p>	18 200
Камертон-2	<p>Блок управления и контроля системой;</p> <p>Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот;</p> <p>Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные рамы, прочие элементы строительной конструкции);</p> <p>Акустоизлучатели разных типов, создающие помехи в акустических каналах утечки данных (вентиляционная система, дверные проемы, трубы инженерных коммуникаций, пр.);</p> <p>Размыкатели проводных линий, перекрывающие утечку акустических сигналов по проводам телефонной связи, локальной компьютерной сети, пр.;</p> <p>Виброшторы, создающие надежную помеху для прослушки разговоров с помощью направленного микрофона через оконное стекло.</p>	46 000

Оптимальным по цене и функционалу без нагромождения сторонних функций оказался ЛГШ-404.

Итоговая цена: 105 300р.

Электромагнитный канал: Активная защита от ПЭМИН

В таблице 3 представлено сравнение средств активной защиты от ПЭМИН.

Таблица 3 - Сравнение средств активной защиты от ПЭМИН

Модель	Функционал	Стоимость, руб
Соната-РЗ.1	<ul style="list-style-type: none"> • исполнение в виде моноблока со встроенной в него антенной; • наличие регулятора уровня излучаемого электромагнитного шума; • наличие специальной проверки; • возможность увеличения уровня излучаемого электромагнитного шума в диапазоне 0.01-100 МГц за счет использования дополнительной антенны (поставляется опционально); • наличие встроенной системы контроля уровня излучения с визуальной и звуковой сигнализацией; • возможность проводного дистанционного управления. 	33120
Гамма-ГШ18	<ul style="list-style-type: none"> • В генераторе установлен счетчик наработки времени с дисплеем (количество часов работы учитывается и прописывается в формуляре изделия); • В генераторе предусмотрена плавная регулировка уровня выходного сигнала (осуществляется встроенным аттенюатором в пределах не менее 20 дБ) • Предназначен для маскировки ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей и комплексов на объектах вычислительной техники 	29 400

Генератор шума "Покров"	<ul style="list-style-type: none"> • исполнение в виде сетевого удлинителя со встроенной антенной; • наличие регулятора уровня излучаемого электромагнитного шума; • независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления; • наличие встроенной системы контроля уровня излучения с визуальной и звуковой сигнализацией; • возможность крепления на вертикальные поверхности и в стойку 19"; • возможна поставка с вилкой IEC C14 для подключения к источнику бесперебойного питания. 	33 900
----------------------------	---	--------

Был сделан выбор в пользу Гамма-ГШ18 как простой в установке и использовании, а также наиболее бюджетный среди аналогов.

Итоговая стоимость: 58 800 рублей.

Защита от закладных устройств

Далее представлена таблица 4, в которой отражено сравнение поисковых антизакладных устройств.

Таблица 4 – Средства защиты от закладных устройств

Модель	Функционал	Стоимость, руб
ST131.S "ПИРАНЬЯ II"	<ul style="list-style-type: none"> • сканирование радиоэфира, проводных и инфракрасного диапазона; • контроль работы систем защиты • виброакустического подавления. 	543 600
ST-167 "Бетта"	<ul style="list-style-type: none"> • простейший поиск источников радиосигнала; • избирательный прием сигнала; 	80 000

	<ul style="list-style-type: none"> • постоянный мониторинг с созданием базы данных событий; • работа по расписанию. 	
Крона-М6	<ul style="list-style-type: none"> • сканирование радиоэфира, проводных • коммуникаций и инфракрасного диапазона; • обнаружение кратковременных сигналов, шумоподобных сигналов; • контроль работы аппаратуры подавления; • автономная работа: до 4 часов. 	1 360 000

Эталонным средством защиты закладных устройств было выбрано средство ST131.S "ПИРАНЬЯ II".

Стоимость: 543 600 рублей.

Подавление сигнала закладных устройств

В таблице 5 приведены средства подавления сигнала закладных устройств.

Таблица 5 – Сравнение средств подавления закладных устройств.

Модель	Функционал	Стоимость, руб
Блокиратор сотовой связи ЛГШ-716	<ul style="list-style-type: none"> • блокировка сотовой связи, Bluetooth, WiFi 2.4 ГГц; • время постоянной работы: не ограничено; • срок службы: 10 лет. 	89 700
Блокиратор стандартов Wi-Fi, Bluetooth ЛГШ-702	<ul style="list-style-type: none"> • блокировка Bluetooth, WiFi 2.4 ГГц; • время постоянной работы: не ограничено; • срок службы: 10 лет. 	61 100
ЛГШ-725	<ul style="list-style-type: none"> • блокировка сотовой связи, Bluetooth, WiFi 2.4 и 5 ГГц; • независимая регулировка мощности по каждому диапазону; • дистанционное управление; • постоянное время работы. 	247 000

Было выбрано решение Блокиратор сотовой связи ЛГШ-716 как более бюджетное среди других моделей этой серии. Стоимость составляет 89 700 рублей.

Подавление микрофонов

Далее на таблице 6 были рассмотрены различные модели (в том числе и отечественные) средств подавления микрофонов.

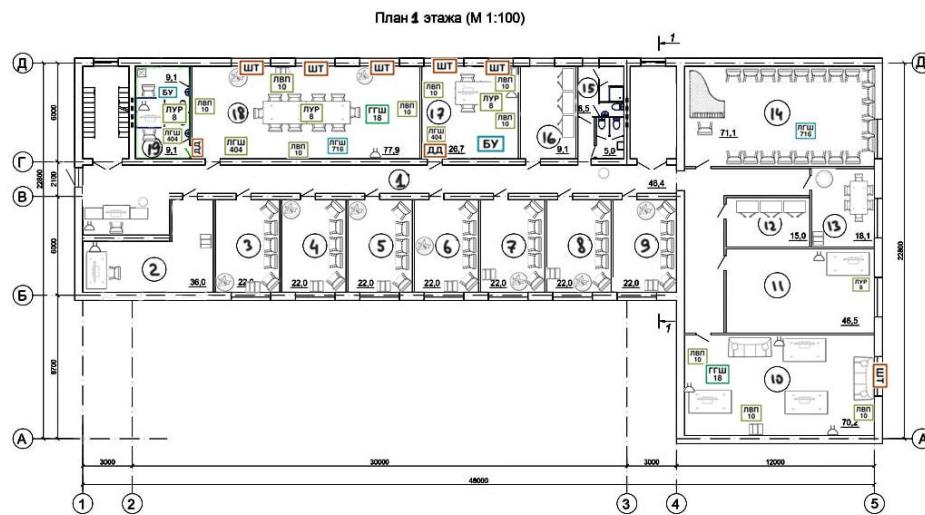
Таблица 6 – сравнение средств подавления сигнала микрофона.

Модель	Функционал	Стоимость, руб
Бубен-Ультра	<ul style="list-style-type: none"> • три типа помех: ультразвуковой диапазон, • сложная звуковая помеха, речеподобная помеха; • возможность автономной работы: до 6 часов; • радиус подавления: до 5 м; • различные варианты маскировки. 	48 000
BugHunter DAudio bda-3 Voices	<ul style="list-style-type: none"> • ультразвуковой диапазон; • автономная работа; • радиус подавления: до 3 м; • дистанционное управление. 	68 900
BugHunter DAudio bda-5	<ul style="list-style-type: none"> • три типа помех: два вида ультразвука, • акустическая помеха; • радиус подавления: до 10 м; • дистанционное управление. 	145 600

Среди аналогов наиболее полным функционалом обладает средство Бубен-Ультра, а также имеет наименьшую стоимость - 48 000 рублей.

Итоговая цена: 96 000.

Далее на рисунке 5 представлен план с размещенными СЗИ.



ШТ - Шторы	ГГШ 18 - Гамма-ГШ18
ДД - Дверной Доводчик	ЛГШ 716 - средство подавления сигналов "ЛГШ-716"
ЛГШ 404 - излучатель виброакустических помех "ЛГШ-404"	БУ - средство подавления микрофонов "Бубен Ультра"
ЛВП 10 - вибровозбудитель "ЛВП-10"	
ЛВП 2А - акустический излучатель "ЛВП-2А"	
ЛУР 8 - размыкатель Ethernet "ЛУР-8"	

Рисунок 5 – План помещения с установкой СЗИ.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы были выполнен анализ имеющихся методов обучения персонала основным необходимым знаниям о мерах информационной безопасности, применяемых на предприятии, а именно дистанционное обучение, аттестация, тренинг и конференция. Данные методы были оценены по критериям стоимости, сроков проведения, повышение репутации компании среди соискателей работы, а также психологическое влияние мер на состояние сотрудников – выявлено влияние групповых занятий на командообразование внутри коллектива.

Также в ходе работы были выявлены оптимальные решения для организаций в зависимости от численности сотрудников – для малого, среднего и крупного бизнеса.

Также в работе отмечено отличие подхода к обучению работников старшего поколения – о необходимости особого подхода при нюансах взаимодействия с новой обстановкой технологических решений.

В заключении раскрывается вопрос о необходимости ознакомления каждого сотрудника с правилами, принятыми компанией и закрепленных Политикой Безопасности организации.

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.
3. Специализированный холдинг. Лаборатория ППШ. URL: <https://labpps.ru> (дата обращения: 11.12.2023).