

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

**По дисциплине:
«Инженерно-технические средства защиты информации»**

**На тему:
«Проектирование инженерно-технической системы защиты информации
на предприятии»**

Выполнил(а):

Семенова Юлиана
Дмитриевна, студентка
группы N34511


(подпись)

Проверил преподаватель:

Попов Илья Юрьевич,
к.т.н., доцент ФБИТ

(подпись)

Отметка о выполнении:

Санкт-Петербург

2023

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

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

Краткие методические указания

Содержание пояснительной записки

Курсовая работа включает разделы:

Введение

1. Общие сведения о защищаемой организации.
2. Перечень управляющих документов.
3. Анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств.
4. Анализ рынка технических средств.
5. Разработка схемы расстановки выбранных технических средств в защищаемом помещении
6. Заключение.

Рекомендуемая литература

-

Руководитель

(Подпись, дата)

Студент

(Подпись, дата)


19.12.2023

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

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

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курс.работу	01.12.2023	01.12.2023	
2	Анализ собранных материалов	05.12.2023	05.12.2023	
3	Написание курсовой работы	14.11.2023	15.11.2023	
4	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель	_____
	(Подпись, дата)
Студент	_____
	 19.12.2023 (Подпись, дата)

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

Студент	Семенова Ю.Д.
Факультет	Безопасности информационных технологий
Группа	N34511
Направление (специальность)	Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Разработать инженерно-техническую систему 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 ☐ Конструирование
☐ Моделирование ☒ Другое: отчёт

3. Содержание работы

В работе представлен результат анализа рынка инженерно-технических средств защиты информации и на его основе разработана инженерно-техническая система защиты информации на предприятии.

4. Выводы

В результате выполнения курсовой работы было проведено обследование НПАО "BLACK.OUT" и разработана инженерно-техническая система защиты информации организации.

Руководитель _____

(Подпись, дата)

Студент _____

19.12.2023

(Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
1. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ.....	7
2. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	9
2.1. Акустический канал.....	9
2.2. Материально-вещественный канал.....	11
2.3. Визуально-оптический канал.....	12
2.4. Электромагнитный канал.....	12
3. ПЕРЕЧЕНЬ УПРАВЛЯЮЩИХ ДОКУМЕНТОВ.....	15
4. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ С ТОЧКИ ЗРЕНИЯ ВОЗМОЖНЫХ УТЕЧЕК ИНФОРМАЦИИ И ТРЕБУЕМЫХ ДЛЯ ЗАЩИТЫ ТЕХНИЧЕСКИХ СРЕДСТВ.....	17
5. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.....	21
6. РАЗРАБОТКА СХЕМЫ РАССТАНОВКИ ВЫБРАННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ В ЗАЩИЩАЕМОМ ПОМЕЩЕНИИ.....	28
ЗАКЛЮЧЕНИЕ.....	32
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ.....	33

ВВЕДЕНИЕ

В организации обрабатываются сведения, содержащие государственную тайну, а именно сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты. Для защиты информации необходимо соответствующе оборудовать помещение и обеспечить защиту от утечки информации путём установки инженерно-технического оборудования.

Целью курсовой работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с грифом «секретно».

Задачи, решаемые в ходе выполнения данной работы:

1. Произвести анализ технических каналов утечки информации;
2. Составить перечень управляющих документов;
3. Произвести анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;
4. Произвести анализ рынка технических средств защиты информации разных категорий;
5. Разработать схемы расстановки выбранных технических средств в защищаемом помещении.

1. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ

Наименование организации: НПАО "BLACK.OUT"

Область деятельности: Аутсорсинг IT-специалистов, занимающихся тестированием в формате Red Team.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

- сведения составляющие государственную тайну;
- информация конфиденциального характера:
 - персональные данные;
 - коммерческая тайна

Информационные потоки и структура организации представлена на рисунке 1.1.

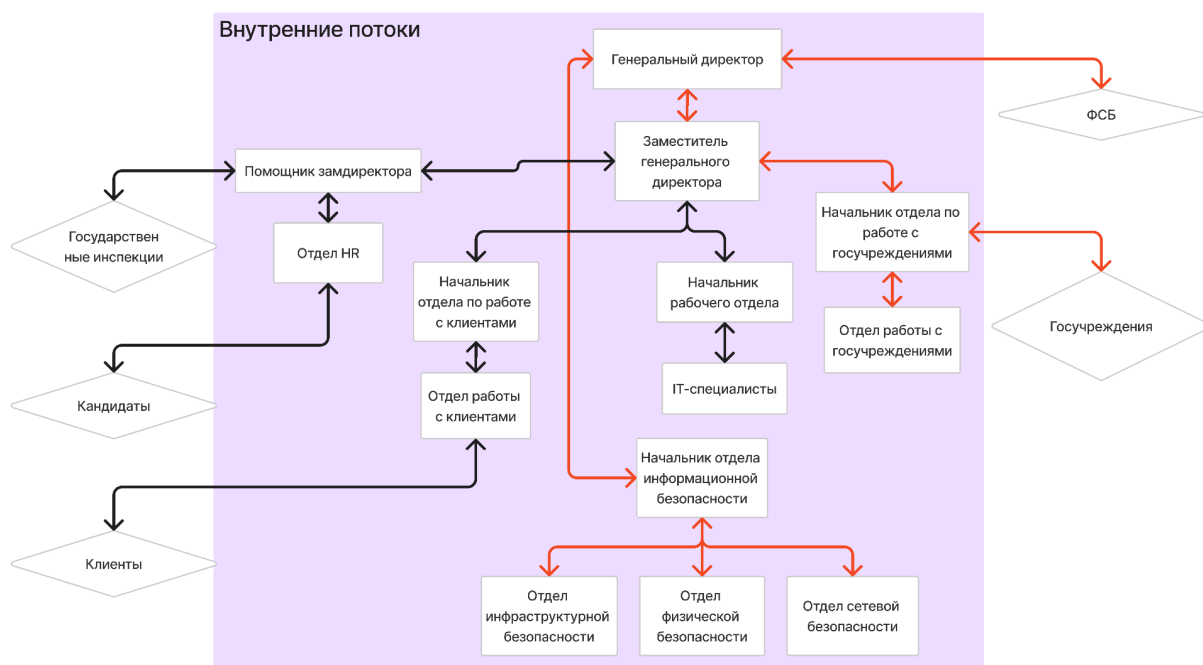


Рисунок 1.1 – Информационные потоки между отделами предприятия и структура

— Закрытый канал связи

— Открытый канал связи

Прибыль, расходы, стоимость информационных активов:

- Прибыль: 70 000 000 рублей/мес
- Расходы:
 - заработная плата сотрудников: 45 700 000 рублей/месяц;
 - коммунальные услуги, интернет, обслуживание здания: 1 000 000 рублей/месяц;

- закупка и обслуживание оборудования и ПО: 5 000 000 рублей/месяц.
- Информационные активы:
 - сведения, составляющие государственную тайну: 2 000 000 000 рублей;
 - персональные данные сотрудников и клиентов: 200 000 000 рублей;
 - коммерческая тайна (структура, планы закупок, планы помещений и т.д.): 300 000 000 рублей.

Персонал организации: 55 человек.

2. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Канал утечки информации – это совокупность источника информации, материального носителя (или среды распространения несущего эту информацию сигнала) и средства выделения информации из сигнала или носителя.

Классификация каналов утечки информации представлены на рисунке 2.1.



Рисунок 2.1 - Классификация каналов утечки информации

2.1. Акустический канал

Акустический канал утечки информации формируется из трех элементов:

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

Акустические каналы утечки информации могут быть следующих видов:

- **прямой акустический** - в прямых акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. В качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический. Перехват акустической (речевой) информации из выделенных помещений по данному каналу может осуществляться: с использованием портативных устройств звукозаписи (диктофонов), скрытно установленных в выделенном помещении, с использованием

электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной среде), скрытно установленных в выделенном помещении, с передачей информации по радиоканалу, оптическому каналу, электросети 220 В, телефонной линии, соединительным линиям ВТСС и специально проложенным кабелям, с использованием направленных микрофонов, размещенных в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных помещениях (непреднамеренное прослушивание).

- **виброакустический** - виброакустический канал состоит из тех же элементов, что и акустический: объект сигнала, среда распространения, агент, принимающий данные. Различие состоит в характеристиках среды. Это не воздух, а строительные и иные конструкции, при прохождении по которым акустический канал создает вибрацию, снимаемую при помощи лазерного луча и преобразованную в информацию.
- **акустоэлектрический** - акустоэлектрические технические каналы утечки информации возникают вследствие преобразования информативного сигнала из акустического в электрический за счет “микрофонного” эффекта в электрических элементах вспомогательных технических средств и систем. Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающим “микрофонным эффектом”, специальных высокочувствительных низкочастотных усилителей (пассивный акустоэлектрический канал)
- **акустооптический** - съем информации осуществляется с плоской поверхности, колеблющейся под действием акустической волны, лазерным лучом в ИК-диапазоне, что обеспечивает невидимость его невооруженным глазом. В качестве поверхности, на которую оказывает воздействие акустическая волна, используется внешнее стекло окна. Стекло облучается источником лазерного излучения с внешней стороны, например из окна соседнего дома. На поверхности соприкосновения лазерного луча со стеклом происходит модуляция лазерного луча акустическими сигналами, генерируемыми в помещении (речь, звуковые колебания работающих технических систем). После отражения от стекла модулированный по амплитуде и фазе лазерный луч принимается приемником ИК-излучения, преобразуется в электрический сигнал и

после соответствующей обработки преобразуется в акустический сигнал, несущий интересующую информацию.

- **параметрический** - образование пассивного акустоэлектро-магнитного канала утечки информации связано с наличием в составе некоторых ВТСС высокочастотных генераторов. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации часто называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а следовательно, к изменению частоты излучения генератора, то есть к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной ёмкости с воздушным диэлектриком в колебательных контурах гетеродинов.

2.2. Материально-вещественный канал

Материально-вещественный канал – каналы утечки информации, возникающие за счет неконтролируемого выхода за пределы контролируемой зоны различных материалов и веществ, в которых может содержаться конфиденциальная информация.

Примеры инцидентов и утечек данных по таким каналам:

- хищение или потеря USB-накопителя;
- передача физических документов.

Защитить важную информацию от утечек по материально-физическим каналам помогут организационные и технические меры. Первые предполагают внедрение системы учета физических носителей и документов, а также допусков к ним, принтерам, копировальной и другой технике с обязательным документированием.

Что касается именно USB-накопителей, эффективный способ защиты — использование средств шифрования данных, хранящихся на них с помощью алгоритмов

AES-256, BlowFish-448 и подобных им. В таком случае, даже если носитель попадает в чужие руки, считать с него информацию не получится.

2.3. Визуально-оптический канал

Возникают при дистанционном считывании и фиксации информации с различных носителей: например, фотографирование дисплеев мониторов, экранов для демонстрации презентаций, бумажных носителей, аудиозапись переговоров и пр. Непосредственно физического контакта с носителем данных в этом случае не происходит.

Для защиты информации от утечки по этим каналам специалисты по информационной безопасности рекомендуют:

- ограничивать доступ сотрудников к визуальной информации. В этом помогут специально разработанные политики безопасности.
- оборудовать помещения, в которых работают с визуальными данными, средствами преграждения или ослабления отраженного света: темными стеклами, шторами, роллетами, ставнями.
- располагать экраны и другие защищаемые объекты так, чтобы исключить отражение света в сторону посторонних лиц.
- применять маскировку объектов и носителей информации. Технологий масса — от управления контрастом фона, на котором демонстрируется защищаемая информация, до применения аэрозольных завес и других специальных решений.

2.4. Электромагнитный канал

Данный канал наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно:

- побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;
- побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
- побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения элементов ТСПИ

В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза)

изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ

В состав ТСПИ могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов, которые излучаются в окружающее пространство.

Побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ

Паразитная генерация в элементах ТСПИ, в том числе, самовозбуждение усилителей низкой частоты (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.), возможна за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе усилителя в нелинейный режим работы, т.е. в режим перегрузки.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;

- запись информации на накопители на магнитных носителях;
- чтение информации с накопителей на магнитных носителях;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства – принтеры, плоттеры;
- запись данных от сканера на магнитный носитель (ОЗУ).

Для перехвата побочных электромагнитных излучений ТСПИ “противником” могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Как правило, полагается, что ТСР ПЭМИН располагаются за пределами контролируемой зоны объекта.

3. ПЕРЕЧЕНЬ УПРАВЛЯЮЩИХ ДОКУМЕНТОВ

Для организованной работы с информацией и её защитой в организации необходимо соблюдать требования следующих нормативных актов:

- Закон РФ от 21.07.93 N 5485-I "О государственной тайне";
- Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) "О коммерческой тайне";
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ;
- Указ Президента РФ от 30 ноября 1995 г. N 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне";
 - сведения, раскрывающие методы, способы или средства защиты информации, содержащей сведения, составляющие государственную тайну, планируемые и (или) проводимые мероприятия по защите информации от несанкционированного доступа, иностранных технических разведок и утечки по техническим каналам, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
 - сведения, раскрывающие методы, средства, организационные, технические или иные меры, направленные на обеспечение режима секретности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.
- Указ Президента Российской Федерации от 06.03.1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера";
- Постановление Правительства РФ от 15 апреля 1995 г. 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";
- Постановление Правительства РФ от 04.09.1995 N 870 (ред. от 30.10.2021) "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности";
- Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51);

- ГОСТ Р ИСО/МЭК 27002-2021 “Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности”;
- Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам связи»(утв. Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51).

4. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ С ТОЧКИ ЗРЕНИЯ ВОЗМОЖНЫХ УТЕЧЕК ИНФОРМАЦИИ И ТРЕБУЕМЫХ ДЛЯ ЗАЩИТЫ ТЕХНИЧЕСКИХ СРЕДСТВ

Для разработки комплекса инженерно-технической защиты информации, необходимо описать выбранные помещения.

План помещения представлен на рисунке 3.1, рисунке 3.2 и 3.3.



Рисунок 3.1 – План 2-го этажа

Легенда:

- лаборатория (1). Здесь находится суперкомпьютер для моделирования системы клиента для нахождения лучшего пути взлома. Также с помощью него происходит перебор ключей для расшифровки необходимых данных;
- кабинет генерального директора (2);
- туалетная комната (3);
- кабинет секретаря (4);
- кабинет отдела безопасности, который занимается документацией и мониторингом (5);
- кабинет HR (6);
- офис для сотрудников, занимающихся работой с госучреждениями (7);
- кабинет начальника отдела безопасности (8), который является администратором ИБ;

- офис для сотрудников по работе с клиентами (9).

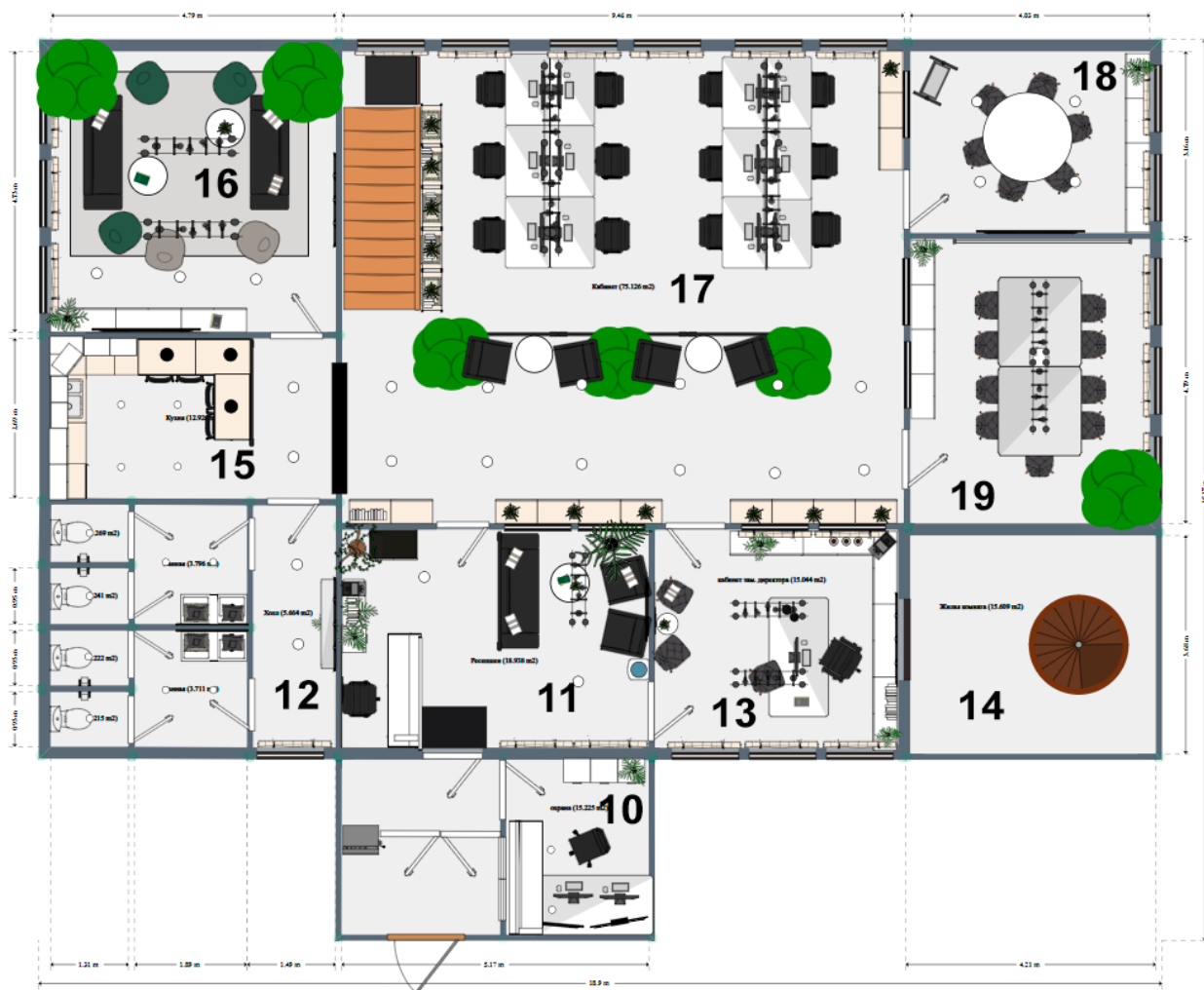


Рисунок 3.2 – План 1-го этажа

Легенда:

- место для охраны (10). Там находится щитовая, видеорегистратор и мониторы, ручное управление СКУДом;
- ресепшн (11). Запись на посещение, учёт времени, направление к начальству;
- туалетная комната (12);
- кабинет заместителя директора (13). Там находится потайная дверь с биометрическим идентификатором по радужке глаза для попадания на винтовую лестницу;
- винтовая лестница (14) для спуска на цокольный этаж;
- кухня (15);
- зона отдыха (16);
- офис для IT-специалистов (17), лестница на 2-ой этаж;
- переговорная (18) для коммерческих предложений;
- переговорная (19) для сотрудников для проведения планерок.

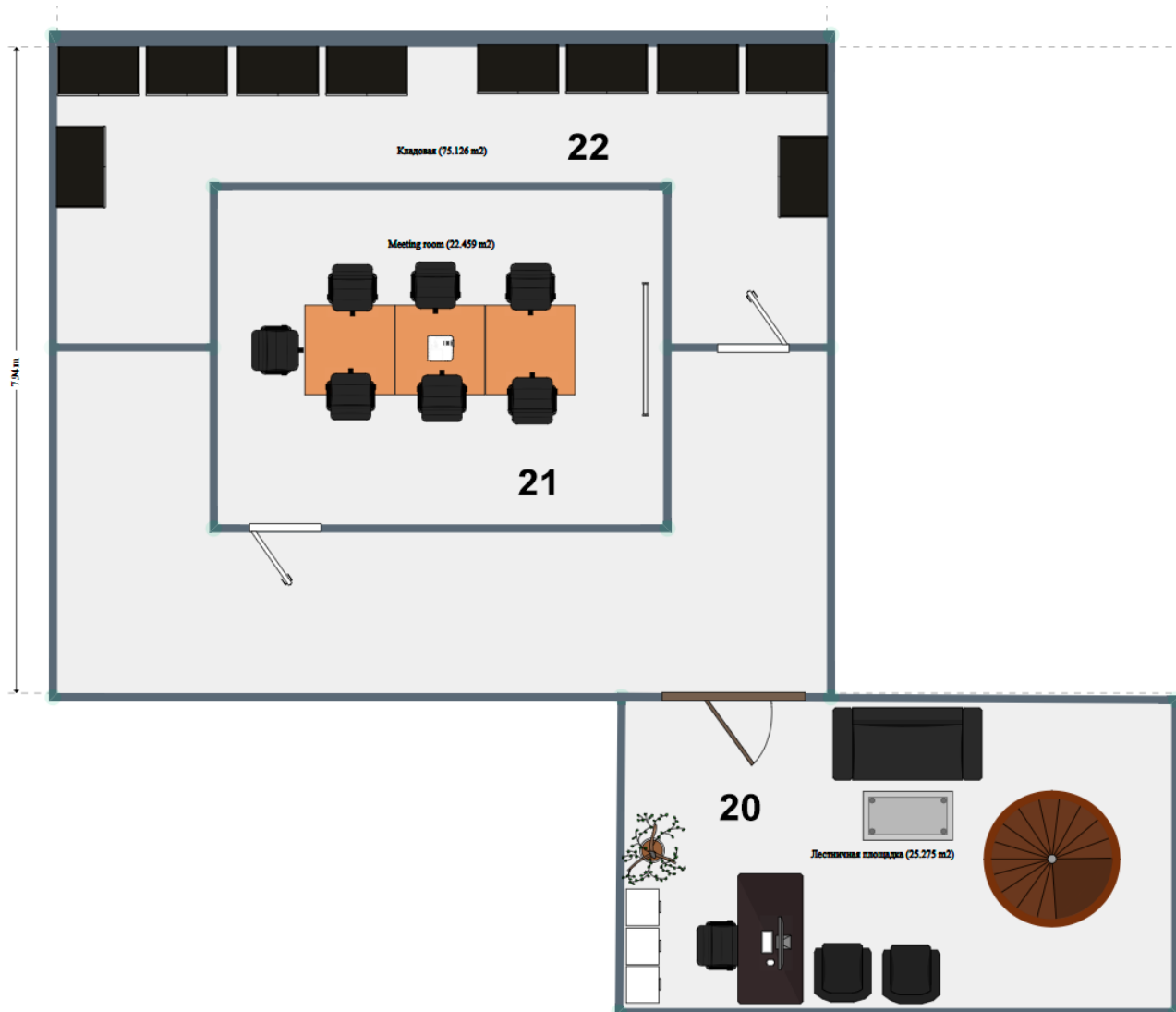


Рисунок 3.3 – План цокольного этажа

Легенда:

- холл с секретарём (20). Учёт посетителей, работа с документами, содержащими сведения государственной тайны;
- переговорная (21) для работы с госучреждениями и для обсуждения сведений, содержащих государственную тайну;
- серверная (22).

Далее представлен результат анализа в виде таблицы 1 с номером защищаемого помещения и возможными каналами утечки информации.

Таблица 1 – Возможные каналы утечки информации

Номер помещения	Каналы утечки					
	Беспроводная и сотовая связь	Акустический канал	Виброакустический канал	ПЭМИН	Слаботочные линии	Оптический канал
1	-	-	-	-	-	-
2	-	+	+	+	+	+
4	+	-	-	+	+	-
5	-	+	+	+	+	+
6	+	-	-	+	+	-
7	-	-	+	+	+	+
8	-	+	+	+	+	+
9	-	+	+	+	+	+
10	-	-	-	+	+	+
11	+	+	-	+	+	+
13	-	+	+	+	+	+
17	+	-	+	+	+	+
18	+	+	+	-	-	+
19	+	+	+	-	-	+
20	+	+	-	+	+	-
21	-	+	+	+	+	-
22	-	-	+	+	+	-

5. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Первым каналом для анализа рынка средств выбран визуально-оптический.

Для защиты визуально оптического канала используются: шторы, рольставни, укрепленные двери, отражающая пленка для окон. Все данные средства ограничивают видимость для злоумышленников, что предотвращает возможные утечки информации по визуально-оптическому каналу. В качестве средства выбрана отражающая пленка для окон и рольставни. Рольставни будут располагаться только на первом этаже здания организации.

Следующим пунктом анализа будут средства акустической и вибрационной постановки помех. Результат анализа представлен в таблице 2.

Таблица 2 - Средства акустической и вибрационной постановки помех

Название устройства	Описание	Цена
ЛГШ-304	Предназначено для защиты акустической речевой информации, путем формирования акустических маскирующих шумовых помех.	25 220 руб.
Буран	Обеспечивает защиту циркулирующей в помещении акустической речевой информации от утечки за счет вибрационных сигналов, возникающих/формируемых под воздействием акустического сигнала на ограждающие конструкции и предметы интерьера, регистрируемых аппаратурой акустической речевой разведки на базе лазеров.	67 500 руб.
СОНАТА АВ-4Б	Соната-АВ” модель 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)" Благодаря этому построению проявляется высокая стойкость защиты информации. Имеет ряд преимуществ перед "классическим" подходом - "центральный генератор + электроакустические преобразователи".	44 200 руб.
ЛГШ-301	Генератор акустического шума ЛГШ-301 предназначен для защиты речевой информации от перехвата по прямому акустическому, виброакустическому и оптикоакустическому каналам. Изделие позволяет защищать речевую информацию, в обычном помещении, оборудованном сетью 220 В. Принцип действия ЛГШ-301 основан на генерации «белого шума» в акустическом диапазоне частот и, как следствие, повышении отношения акустическая помеха/речевой сигнал. Генератор защищает пространство объемом до 50 куб. м. Если Вы работаете в большом помещении, необходимо использовать несколько генераторов. Диапазон рабочих частот: 180-11300 Гц.	8 160 руб.

Название устройства	Описание	Цена
ЛГШ-404	Изделие предназначено для защиты акустической речевой информации, циркулирующей в помещениях, специально предназначенных для обсуждения или воспроизведения с помощью средств звукоусиления речевой информации, составляющей государственную тайну, или в помещениях, оборудованных средствами правительственной связи, иных видов специальной связи, а также в помещениях, предназначенных для проведения мероприятий с обсуждением информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки информации по виброакустическому и акустическому каналам.	35 100 руб.

В ходе анализа рынка средств акустической и вибрационной защиты было выбрано средство производства Лаборатории ППШ ЛГШ-404, данное средство является средством активной защиты.

Далее будет представлен список средств для блокирования беспроводной и сотовой связи. Результат анализа представлен в таблице 3.

Таблица 3 - Средства для блокирования беспроводной и сотовой связи

Название устройства	Описание	Цена
ЛГШ-725	Блокиратор является новой модификацией популярного генератора ЛГШ-719 с дополнительным подавлением сигналов WiFi на частоте 5 ГГц. Блокиратор сотовой связи ЛГШ-725 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах: <ul style="list-style-type: none"> - IMT-MC-450; - GSM900; - DSC/GSM1800, (DECT1800); - IMT-2000/UMTS (3G); - LTE 2600 (4G, WiMAX); - LTE 800 (4G); - Bluetooth; - WiFi 2.4 ГГц; - WiFi 5 ГГц. 	247 000 руб.
ЛГШ-702	Блокиратор работы устройств, работающих в стандартах: <ul style="list-style-type: none"> - Bluetooth - WiFi Изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания,	61 100 руб.

Название устройства	Описание	Цена
	несанкционированной передачи данных, а также, для блокирования работы радиоисполнительных устройств, созданных с использованием стандартов Bluetooth и WiFi.	
ЛГШ-701	Изделие ЛГШ-701 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи работающих в стандартах: <ul style="list-style-type: none"> - IMT-MC-450(NMT-450i); - GSM900; - E-GSM900 - DSC/GSM1800 - DECT1800 - CDMA2000 1x 	97 500 руб.
ЛГШ-703	Изделие ЛГШ-703 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандарте IMT-2000/UMTS. Кроме того, изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, созданных на основе сотовых телефонов. В результате работы изделия происходит потеря сети оператора сотовой связи пользовательским терминалом и возвращение в нормальный режим работы после выключения изделия.	97 500 руб.

В ходе анализа были выбраны два средства производства Лаборатории ППШ: ЛГШ-702 и ЛГШ-701. Выбраны два средства, чтобы заблокировать, как стандарты Bluetooth и Wi-Fi, так и стандарты сетей сотовой связи. Они являются средствами активной защиты.

Необходимо также обеспечить защиту от ПЭМИН. Для этого необходимо проанализировать средства пространственного зашумления. Анализ представлен в таблице 4.

Таблица 4 - Средства пространственного зашумления

Название устройства	Описание	Цена
ЛГШ-501	<p>Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-501» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <p>Напряжение шумового сигнала - 0,01 - 400 МГц; 10 - 58 дБ. Электрическое поле - 0,01 - 1800 МГц; 15 - 75 дБ. Магнитное - 0,01 - 30 МГц; 20 - 65 дБ.</p>	29 900 руб.
ЛГШ-503	<p>Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-503» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <p>Напряжение шумового сигнала - 0,01 - 400 МГц; 10 - 58 дБ. Электрическое поле - 0,01 - 1800 МГц; 15 - 75 дБ. Магнитное - 0,01 - 30 МГц; 20 - 65 дБ.</p>	44 200 руб.
СОНАТА-ФС 10.1	<p>СЗИ помехоподавляющий сетевой фильтр "Соната-ФС10.1", предназначен для защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных наводок информативного сигнала на линии электропитания напряжением 220 В с частотой 50 Гц.</p>	50 400 руб.
ЛГШ-513	<p>Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-513» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p>	39 000 руб.

Лучшим средством для постановки пространственных помех в ходе анализа выбрано средство производства Лаборатории ППШ ЛГШ-513, что является средством активной защиты.

Следующими средствами защиты для анализа выбраны средства защиты слаботочных линий и линий связи. Результат анализа представлен в таблице 5.

Таблица 5 - Защита слаботочных линий и линий связи

Название устройства	Описание	Цена
ЛУР 2	Размыкатель слаботочных линий питания	5 590 руб.
ЛУР 4	Размыкатель слаботочных линий Телефон	5 590 руб.
ЛУР 8	Размыкатель слаботочных линий Ethernet	5 590 руб.
Буран-К1	Размыкатель аналоговых телефонных линий	3 400 руб.
Буран-К2	Размыкатель линий оповещения и сигнализации	3 400 руб.
Буран-К3	Размыкатель компьютерных сетей	3 500 руб.

Лучшими средствами для постановки пространственных помех в ходе анализа выбрано средства производства Лаборатории ПППШ ЛУР 2 и ЛУР 8, так как они входят в состав ЛГШ-404, а данное средство выбрано лучшим средством акустической и вибрационной постановки помех. ЛУР 4 не выбран, так как в организации отсутствуют слаботочные линии Телефон. Данные средства являются средствами пассивной защиты.

Последними для анализа выбраны средства защиты сети переменного тока. Результат анализа представлен в таблице 6.

Таблица 6 - Средства защиты сети переменного тока

Название устройства	Описание	Цена
ЛФС-10-1 Ф	Фильтр сетевой помехоподавляющий ЛФС-40-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц. Предельное значение тока, при котором допускается эксплуатация изделия 10 А.	47 060 руб.
ЛФС-40-1 Ф	Фильтр сетевой помехоподавляющий ЛФС-40-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам	70 200 руб.

Название устройства	Описание	Цена
	побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц. Предельное значение тока, при котором допускается эксплуатация изделия 40 А.	
ЛФС-200-3 Ф	Фильтр сетевой помехоподавляющий «ЛФС-200-3Ф» предназначен для использования в целях защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 380 В с частотой 50 Гц. Предельное значение тока, при котором допускается эксплуатация изделия 200 А.	377 000 руб.
ЛГШ-221	Сетевой генератор шума «ЛГШ-221» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок путем формирования маскирующих шумоподобных помех.	36 400 руб.
СОНАТА-РСЗ	Сетевой генератор шума СОНАТА-РСЗ - средство активной защиты конфиденциальной информации от утечки по проводам электросети. Это устройство предназначено для использования в помещениях, в которых на электронно-вычислительных машинах обрабатываются данные, являющиеся коммерческой либо государственной тайной.	32 400 руб.

В ходе анализа в качестве средств защиты сети переменного тока выбраны средства производства Лаборатории ПППШ: ЛГШ-221, как средство активной защиты и ЛФС-40-1Ф, как средство пассивной защиты.

В итоге в ходе анализа рынка технических средств были выбраны:

1. Средства акустической и вибрационной постановки помех: средство производства Лаборатории ПППШ ЛГШ-404, активная защита.
2. Средства для блокирования беспроводной и сотовой связи: средства производства Лаборатории ПППШ: ЛГШ-702 и ЛГШ-701, активная защиты.
3. Средства пространственного зашумления: средство производства Лаборатории ПППШ ЛГШ-513, активная защиты
4. Защита слаботочных линий и линий связи: средства производства Лаборатории












ППШ ЛУР 2 и ЛУР 8, пассивная защита.

5. Средства защиты сети переменного тока: средства производства Лаборатории ППШ: ЛГШ-221, как средство активной защиты и ЛФС-40-1Ф, как средство пассивной защиты.
6. Средства защиты визуально-оптического канала: отражающая пленка для окон и рольставни, пассивная защита

6. РАЗРАБОТКА СХЕМЫ РАССТАНОВКИ ВЫБРАННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ В ЗАЩИЩАЕМОМ ПОМЕЩЕНИИ

На основе результатов анализа плана помещения предприятия и результатов анализа рынка инженерно-технических средств защиты информации была разработана инженерно-техническая система защиты информации для предприятия НПАО “BLACK.OUT”. Легенда для средств защиты представлена в таблице 7.

Таблица 7 – Легенда

Графическое обозначение	Сокращение	Определение
	СПА	Система постановки акустических помех
	СПВ	Система постановки виброакустических помех
	ББС	Блокиратор беспроводной связи
	БСС	Блокиратор сотовой связи
	СФ	Сетевой фильтр
	СГШ	Сетевой генератор шума
	ГПШ	Генератор пространственного зашумления
	РЕ	Размыкатель Ethernet
	РС	Размыкатель слаботочной линии
	ОП	отражающая пленка для окон
	Р	Рольставни

Состав и размещение инженерно-технических средств защиты информации представлен на рисунке 5.1, 5.2 и 5.3.

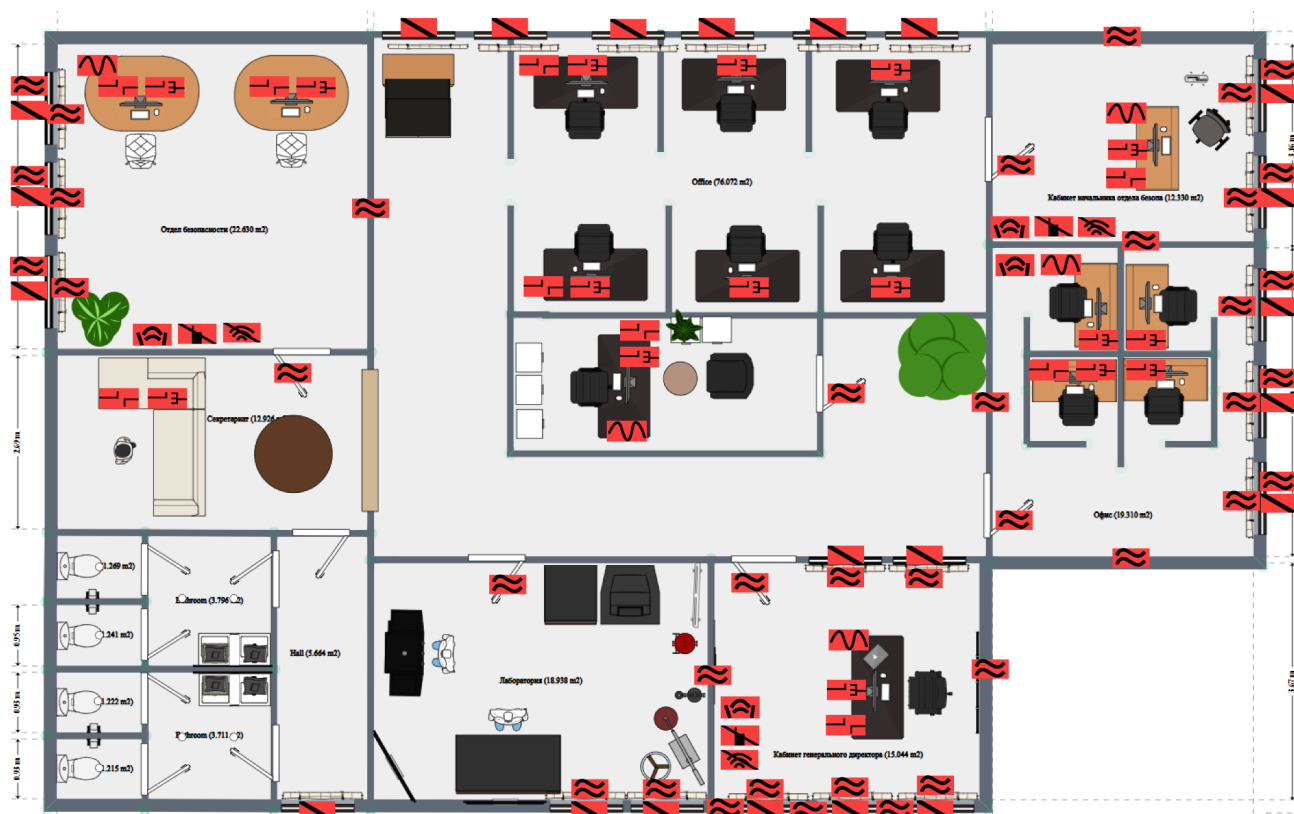


Рисунок 5.1– План для 2-го этажа

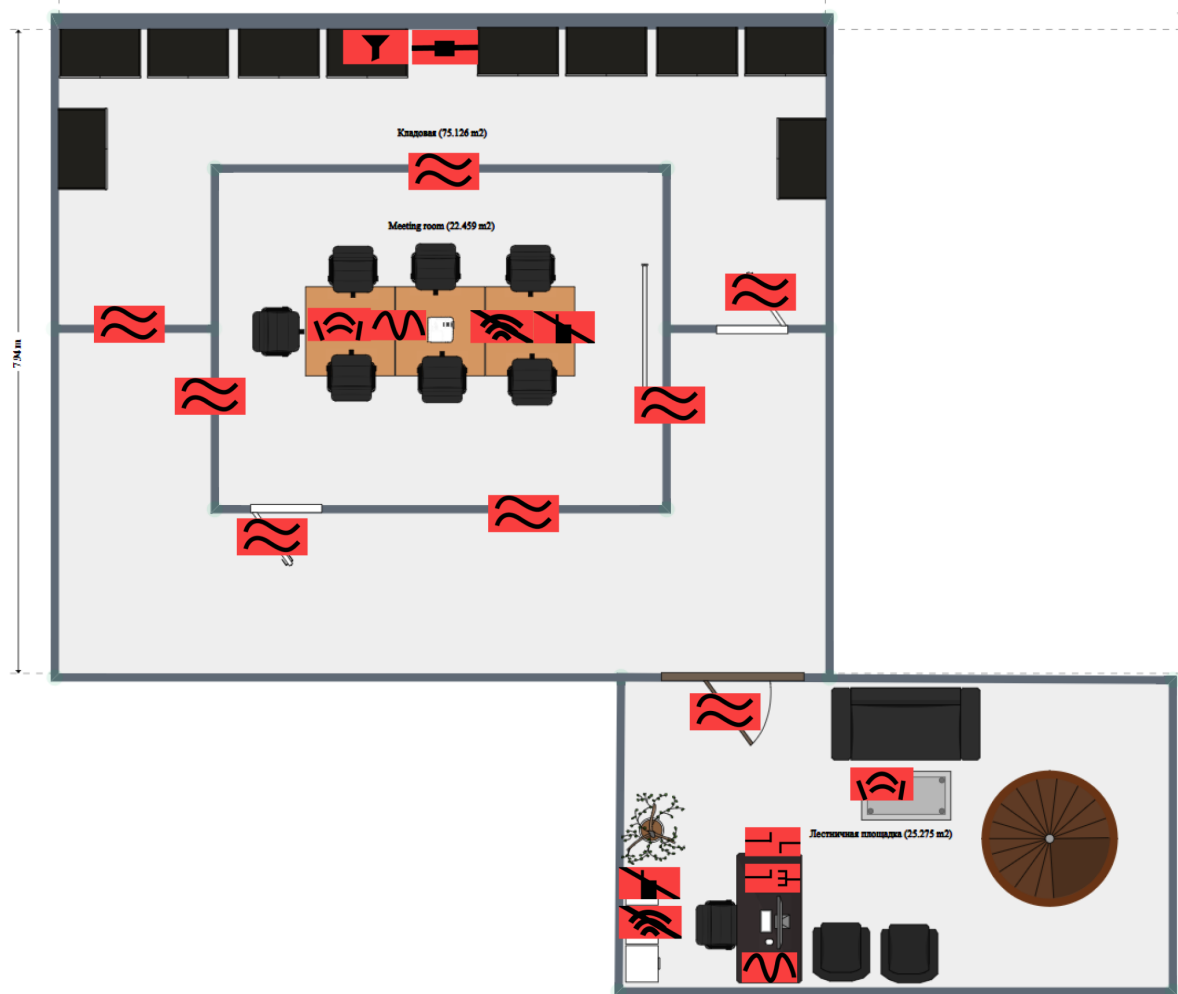


Рисунок 5.3— План для цокольного этажа

ЗАКЛЮЧЕНИЕ

В ходе исследования был осуществлен анализ технических каналов утечки информации предприятия НПАО “BLACK.OUT”, что позволило выявить потенциальные уязвимости в системе безопасности. Произведено обследование организации с целью выявления существующих проблемных зон и определения особенностей рабочего процесса, влияющих на безопасность информации.

На основе проведенного анализа был составлен перечень руководящих документов, регламентирующих вопросы безопасности информации на предприятии. Также было предоставлено обоснование необходимости внедрения и совершенствования мер по защите информации в соответствии с принятыми нормами и стандартами.

Одним из важных этапов работы стал анализ рынка технических средств, предназначенных для обеспечения безопасности информации. Полученные данные позволили выявить актуальные технологии в этой области, что послужило основой для выбора оптимальных средств и методов защиты.

В результате интеграции всех проведенных исследований и аналитических данных была разработана инженерно-техническая система защиты информации.

Результаты исследования предоставляют основу для последующих шагов по внедрению инженерно-технической системы защиты информации на предприятии, что способствует повышению общего уровня безопасности и уверенности в защищенности конфиденциальных данных.

Цель работы достигнута, все задачи выполнены.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Лаборатория ПППШ URL: <http://www.pps.ru/> (дата обращения: 5.12.2023).
2. Detector Systems URL: <https://detsys.ru/> (дата обращения: 5.12.2023).
3. Постановление Совета Министров – Правительства РФ "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам" от 15.09.1993 № 912-51.
4. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1.