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

Факультет безопасности информационных технологий

Дисциплина:

«Организация и управление службой информационной безопасности»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Инженерно-технические средства защиты информации»

Выполнил:

студент группы N34511

Меклерис К.А

_____
(подпись)

Проверил:

доцент ФБИТ, кандидат технических наук

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 Меклерис К.А
(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 Разработка комплекса инженерно-технической защиты информации в помещении

Задание Разработать комплекс 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 курсовой работы представлен в методических пособиях;
3. Объект исследования курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

Введение;

1. Анализ защищаемых помещений;
2. Руководящие документы;
3. Анализ технических каналов утечки информации;
4. Анализ рынка технических средств;
5. Описание расстановки технических средств

Заключение;

Список литературы.

Рекомендуемая литература

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 18.12.2023 г.

(Подпись, дата)

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

Студент Меклерис К.А
(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 Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Заполнение задания на курсовую работу	01.10.2023		
2.	Анализ информации	03.11.2023		
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2023		
4.	Защита курсовой работы	19.12.2023		

Руководитель
(Подпись, дата)

Студент 18.12.2023 г.
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Меклерис К.А (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	Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	Повышение защищенности помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки и выбор мер защиты информации.
2. Характер работы	Конструирование
3. Содержание работы	
Курсовая работа включает разделы:	
Введение	
1. Анализ защищаемых помещений	
2. Руководящие документы	
3. Анализ технических каналов утечки информации	
4. Анализ рынка технических средств	
5. Описание расстановки технических средств	
Заключение	
Список литературы	
4. 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 18.12.2023 г.
(Подпись, дата)

СОДЕРЖАНИЕ

- ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

С наступлением XXI века по всему миру наблюдалась и продолжает развиваться тенденция перехода к постиндустриальному обществу. В данный момент в мире информация является наравне с материальными благами таким же ценным ресурсом. Информация — это сведения о людях, фактах, событиях, явлениях и процессах, независимо от того, в какой форме они выражены. Во все времена владение информацией было выгодно стороне, обладающей более точной и обширной информацией, особенно когда речь идет о конкурентах.

Проблема защиты информации существовала всегда, но сегодня она приобретает особую актуальность в связи с бурным развитием науки и техники. Поэтому задача специалиста по защите информации - овладеть всеми приемами и методами защиты информации, научиться моделировать и проектировать системы защиты информации.

Целью данной работы является описание и построение наиболее полной модели защищаемого объекта. Представлен перечень информации, подлежащей защите, ее носители, вероятность утечки, технические пути утечки, проведено моделирование угроз информационной безопасности.

Цель данной работы - научиться комплексно и целостно анализировать объект защиты, чтобы выявить наиболее опасные пути утечки информации, а также разработать проект по установке инженерно-технических средств защиты информации.

Задачи, выполняемые в работе:

1. Определение в помещении приоритетных мест к защите;
2. Оценка каналов утечки информации;
3. Выбор и размещение мер пассивной и активной защиты информации.

1 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

1.1 Общие сведения об организации

Организация, для которой разработан проект по обеспечению инженерно-технических средств информации – ООО «Чииииз».

Данная организация предоставляет услуги по изготовлению фото для документов. Является негосударственной структурой. Необходимо обеспечить защиту коммерческой тайны, персональных данных. Необходимо обеспечить защиту информации в контексте бизнеса.

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

1.2 Информационные потоки организации

На рисунке 1 представлены информационные потоки организации.

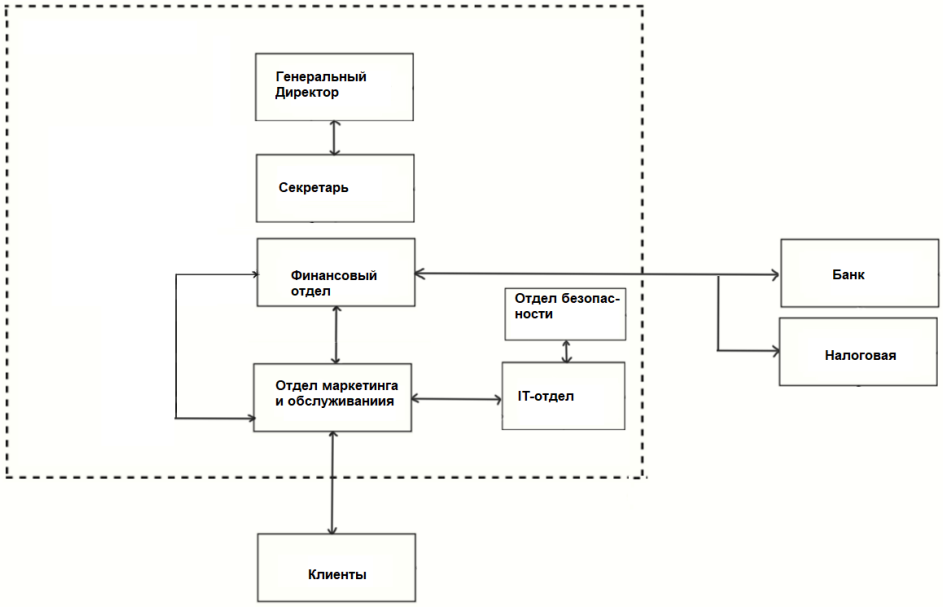

Рисунок 1 – схема информационных потоков ООО «Чииииз»

1.3 Помещение организации

Помещение организации расположено на 5 этаже малого торгового комплекса. Окна расположены на северной, восточной, южной сторонах. Северные окна нуждаются в защите, так как находятся в кабинете директора и в переговорной. Восточные окна выходят в кухню, не нуждаются в особой защите. Южные окна частично нуждаются в защите – только для помещения работы с клиентами.

Доступ к помещению контролируется секцией ресепшена. Допуск в общие

помещения имеют все клиенты и члены организации – к таким помещениям относятся комнаты 4, 5, 6,7, 8.

Допуск к помещениям генерального директора, секретаря, переговорной имеют только члены администрации: генеральный директор, секретарь, администратор. Ограничение доступа осуществлено в виде смарт-замка.

Помещение состоит из:

1. Кабинета директора;
2. Кабинета секретаря;
3. Переговорной;
4. Уборной;
5. Обеденной;
6. Гардероба;
7. Общего коридора;
8. Фотозоны.

Далее на рисунке 2 представлен план помещения.

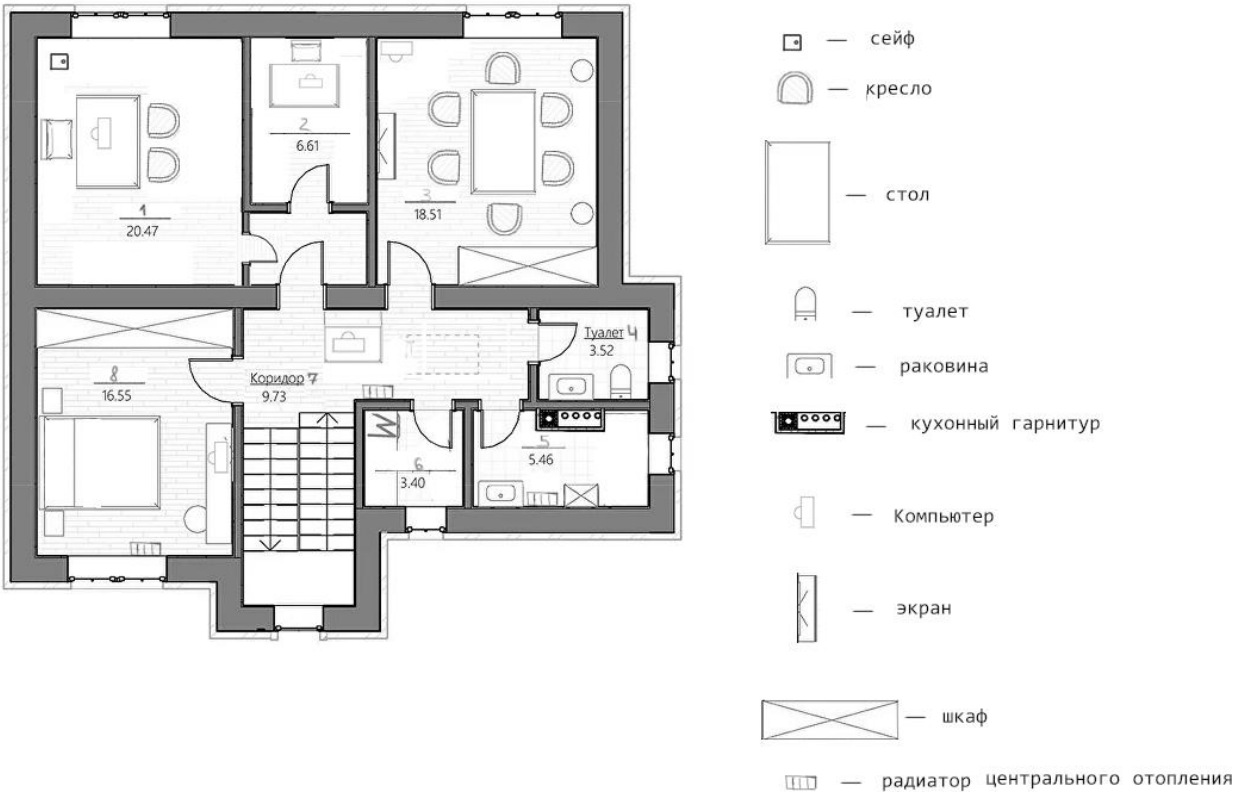

Рисунок 2 – Схема помещения ООО «Чииииз» с условными обозначениями

В организации стоят 5 компьютеров, соединенные локальной сетью и подключенные к сети Интернет.

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

○ 2.1 Перечень руководящих документов

При разработке комплексного проекта по защите информации были учтены следующие документы:

- Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1;
- Федеральный Закон No149 - “Об информации, информационных технологиях и защите информации”;
- постановление Правительства РФ от 26 июня 1995 г, No608 “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”;
- Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ;
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.

3 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Переходя к определению необходимых мер защиты, необходимо обратиться к классификации каналов утечки информации по способу перехвата:

1. Оптический канал;
2. Акустический канал;
3. Электромагнитный канал;
4. Закладные устройства;

3.1 Оптический канал

К данному каналу относятся такие утечки информации как подглядывание с улицы, визуальный съем информации через окна и двери.

Так как помещение находится на 5 этаже торгового комплекса, такая угроза маловероятна, но возможна.

3.2 Акустический канал

К данному каналу относится подслушивание, которое может быть осуществлено со стороны окон с помощью направленного микрофона и лазера. Такие утечки возможны от окон, центрального отопления и стен.

Так как помещение находится на 5 этаже, снятие информации со стен маловероятно. Необходимо обратить внимание на радиаторы отопления и окна.

3.3 Электромагнитный канал

Каждая комната оснащена розетками, ethernet-кабелем. Работа с конфиденциальной информацией происходит на компьютере ресепшена, генерального директора, секретаря, переговорной, в зоне клиентского обслуживания.

3.4 Закладные устройства

Закладное устройство может быть размещено во многих местах клиентского доступа: шкафчики, кухонный гарнитур, клиентская зона. Также возможен пронос в переговорную, подбрасывание под стол ресепшена.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

В данном разделе будут приведены сравнительные таблицы возможных решений по закупке средств защиты информации.

4.1 Оптический канал утечки информации

Для защиты окон в клиентской зоне необходимо установить обычные не просвечивающиеся шторы. Для защиты переговорной и кабинета директора необходимо поставить шторы-блэкаут, полностью ограничивающие возможность оптического снятия информации.

В таблице 1 приведен пример закупки штор для организации.

Таблица 1 – Закупка штор

Наименование	**Стоимость**	**Количество**
Штора на ленте «Рим» 200х310 см цвет серый	1 984₽/шт	1
Штора рулонная блэкаут Inspire Natal 160х190 см светло-серая Granit 5	3 800₽/шт	2

Итоговая сумма: 9584 рубля.

Также на охраняемые помещения необходимо установить дверные доводчики. В таблице 2 представлен вариант закупки доводчиков, детальный разбор аналогов не требуется.

Таблица 2 – Закупка доводчиков

Наименование	**Стоимость**	**Количество**
Доводчик дверной Dorma TS Nano Size 2 максимальная нагрузка 40 кг алюминий цвет черный	1 555₽/шт	4

Итоговая сумма: 6220 рубля.

4.2 Виброакустический канал

Для данного раздела необходимо отдельно рассмотреть звукоизоляцию стен и пола, а также устройства излучения помех, данные о варианте закупки приведены в таблице 3.

Таблица 3 – Закупка обшивки

Наименование	**Стоимость**	**Количество**
Звукоизоляция пола с установкой	4500 /м ^2	39 м^2
Звукоизоляция стен с установкой	4000 / м	51 м
Звукоизолирующие двери с установкой	50 000 р /шт	3

Итоговая сумма: 529 500 рублей.

Далее в Таблице 4 приведены данные о вариантах приборов излучателей помех.

Таблица 4 – Закупка излучателей помех

Наименование	**Сравнение**	**Стоимость**
КАМЕРТОН-5	1 класса защиты (для выделенных помещений до 1 категории включительно, не оборудованных системами звукоусиления); 2 класса защиты (для выделенных помещений до 2 категории включительно, оборудованных системами звукоусиления); предназначена для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам	46 000
ЛГШ-404	– учет времени работы; – контроль и защита органов регулировки уровня выходного шумового сигнала; – проводное дистанционное управление и контроль; – диапазон частот: 175 - 11 200 Гц; – круглосуточная непрерывная работа; – средний срок службы: 7 лет.	35 100
ЛГШ-402	Электронные или акустические стетоскопы для прослушивания через потолки, полы и стены. Оснащено визуальной системой индикации нормального режима работы. Проводные или радиомикрофоны, установленные на ограждающие конструкции или водопроводные и отопительные трубопроводы; Лазерные или микроволновые системы съема информации через оконные проемы помещений.	18 200

Оптимальным решением по цене и функционалу является ЛГШ-404. При выборе была учтена необходимость регулировки уровня шумового сигнала.

Итоговая сумма: 70 200 рублей

4.3 Электромагнитный канал

В таблице 5 приведены несколько приборов по защите от Побочных Электромагнитных Излучений и Наводок.

Таблица 5 – Приборы защиты от ПЭМИН

Наименование	**Сравнение**	**Стоимость**
Соната-ФС10.1	Защищаемая линия электропитания Однофазная, номинальное напряжение 220 В, Частота 50 Гц Предельное значение тока нагрузки, не более 10 А	50 400

	Величина реактивного тока, потребляемого ненагруженным фильтром, не более 0,04 А Кабель для подключения 4х1,5 мм2 с двойным экраном Длина кабелей для подключения в стандартной комплектации, не менее2) 2 отрезка по 5 м Заземление 2 болта М5 на корпусе	
ФП-6	для ослабления сигналов наводок и побочного излучения в диапазоне частот 0.01 МГц… 1.8 ГГц. подходит для электроцепей: число фаз - 1; число проводов - 2; напряжение - 220 В; номинальный ток - 20 Ампер. Наряду с ПЭМИН ФП-6 подавляет и любые другие сетевые помехи, тем самым защищая технику от их пагубного воздействия. Уровень затухания помеховых сигналов при прохождении через фильтр достигает 60 дБ.	58 740
ЛФС-10-1Ф	Напряжение питания 220 В Вес 5 Кг Габариты (не более) 310 х 110 х 85 мм Количество фаз защищаемой линии электропитания 1 Длина экранированных кабелей для подключения основного блока к защищаемым линиям электропитания не менее 5 м.	47 100

Сравнивая аналоги, критических отличий между техническими характеристиками не было выявлено, поэтому выбор был сделан в пользу ЛФС-10-1Ф, как более бюджетный вариант.

Итоговая сумма: 94 200 рублей.

4.4 Защита от закладных устройств

Далее в таблице 6 приведены устройства по защите от закладных устройств.

Таблица 6 – Приборы защиты от закладных устройств

Наименование	**Характеристики**	**Стоимость**
ЛГШ-725	**Блокиратор сотовой связи** блокировка сотовой связи, Bluetooth, WiFi 2.4 ГГц; время постоянной работы: не ограничено; срок службы: 10 лет.	247 000
ЛГШ-702	Блокиратор стандартов Wi-fi, Bluetooth блокировка Bluetooth, WiFi 2.4 ГГц; время постоянной работы: не ограничено; срок службы: 10 лет.	61 100
ЛГШ-716	Блокиратор беспроводной связи стандартов: IMT-MC-450 GSM900 DSC/GSM1800, (DECT1800) IMT-2000/UMTS (3G) Bluetooth, WiFi	89 700

Сравнивая технические характеристики и учитывая контекст организации, для которой разрабатывается проект, достаточным решением является ЛГШ-716.

Итоговая сумма: 89 700 рублей.

Также последним пунктом защиты конфиденциальной информации от кражи и НСД является защита от микрофонов, подслушивающих устройств. В таблице7 приведены решения защиты от микрофонов.

Таблица 7 – Средства защиты от микрофонов и диктофонов

Наименование	**Характеристики**	**Стоимость**
BugHunter DAudio bda-5	эффективное устройство в в форме панели, монтируется на стену или потолок; ультразвуковая помеха генерируется сразу сотней мощных излучателей; речеподобная акустическая помеха с "белым" шумом усиливает эффективность;	145 600

	блокирует работу любых устройств с микрофонами, даже профессиональных; безопасен для людей, не вызывает головных болей и проблем со здоровьем; в комплект поставки прибора входят 2 пульта ДУ и сетевой адаптер питания.	
КАНОНИР-К7	Кроме встроенного динамика имеет выход на колонки, что позволяет защититься даже от лазерных микрофонов	37 000
Бубен-Ультра	три типа помех: ультразвуковой диапазон, сложная звуковая помеха, речеподобная помеха; возможность автономной работы: до 6 часов;	48 000

В качестве достаточного и эффективного средства был выбран прибор Канонир К-7.

Итоговая сумма: 74 000 рублей.

4 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Рассмотрев ранее и выбрав оптимальные устройства для разрабатываемого проекта комплексной защиты информации для ООО «Чииииз», был сформирован план расстановки технических средств на периметре организации.

Далее на рисунке 2 представлен проект по обеспечению информационной безопасности для помещения фотостудии.

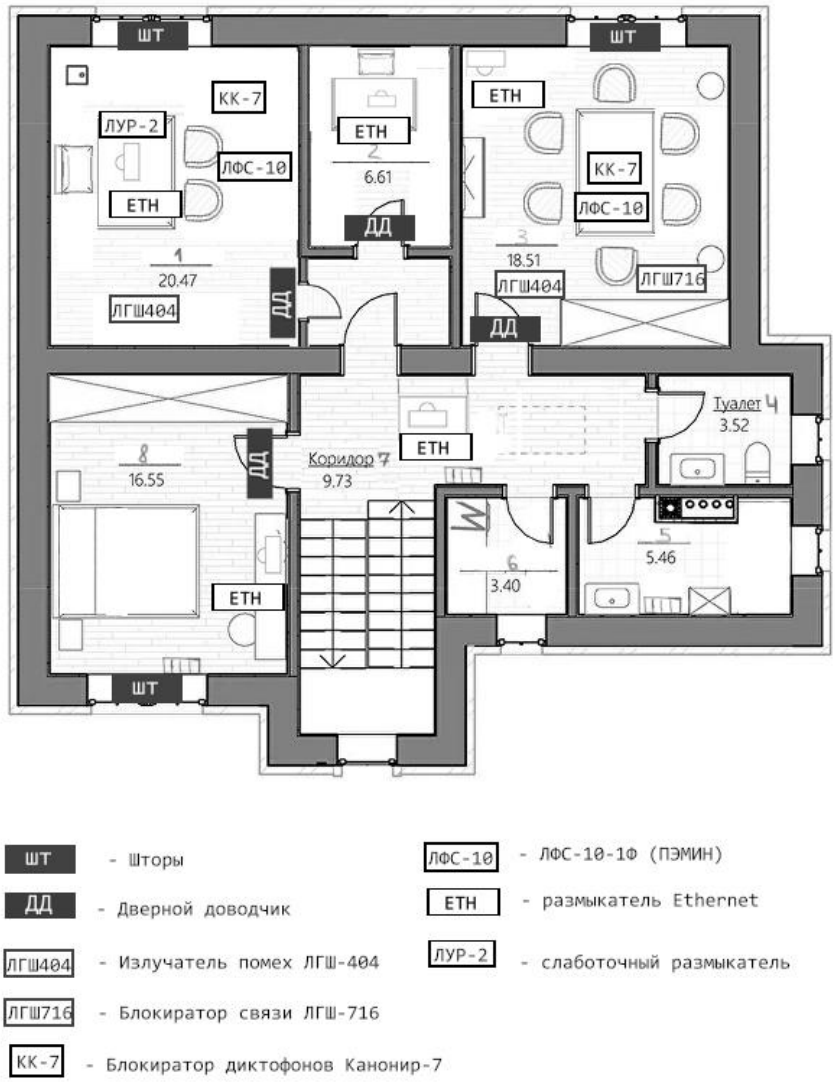

Рисунок 2 – план помещения с нанесенными техническими средствами

Итоговая сумма проекта составляет 873 404 рубля.

Также к проекту можно добавить профилактическое средство от закладных устройств, если бюджет организации расположен к комплексной защите - ST131.S "ПИРАНЬЯ II", стоимость которого составляет 543 600 рублей. Итоговая сумма: 1 417 004 рубля.

ЗАКЛЮЧЕНИЕ

В ходе работы были выделены 4 канала возможных утечек информации. Для каждого канала утечек были рассмотрены устройства защиты, которые снижают риск утечек. Каждый из этих устройств имеет свои уникальные особенности и цели, что позволяет организации выбирать наиболее подходящий в зависимости от своих конкретных потребностей и целей.

Проект инженерно-технических средств защиты, разработанный в рамках данной работы, структурирован по каналам утечки. Эти уровни обеспечивают комплексное измерение эффективности работы службы информационной безопасности, учитывая как общие стратегические аспекты, так и более конкретные процессы и моменты мониторинга.

Таким образом, разработанный проект предоставляет организации все необходимые устройства для систематической работы службы информационной безопасности. Применение данного проекта позволит организации «Чиииз» достичь более высокого уровня защиты информации, выстроив высокие доверительные отношения с компаниями-партнерами и клиентами фирмы.

Итоговая сумма проекта составляет 1 417 004 рубля.

Цель, поставленная в начале работы, достигнута, задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Новая кибербезопасность: от процесса к понятному результату // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/new-cybersecurity-from-process-to-result (дата обращения: 01.11.2023).
2. Оценка эффективности и метрики ИБ // Information Security URL: https://lib.itsec.ru/articles2/control/ocenka-effektivnosti-i-metriki-ib (дата обращения: 01.11.2023).
3. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б. - М.:ЦИПСиР, 2011. - 373 с. ISBN 978-5-9614-1364-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/556539 (дата обращения: 01.11.2023).