Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

Курсовая работа

«Проектирование инженерно-технической системы защиты информации на предприятии»

Вариант 5

Выполнила:

Кунгурова Арюна Александровна,

студент группы N34461

(подпись)

Проверил:

Попов Илья Юрьевич,

к.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Кунгурова Арюна Александровна

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34461

Направление (специальность) 10.03.01. - Технологии защиты информации

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

Задание Проанализировать всевозможные каналы утечки информации в помещении, провести анализ рынка технических средств защиты информации разных категорий, спроектировать план расстановки выбранных технических средств в защищаемом помещении

Краткие методические указания

Рекомендуемая литература

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Кунгурова Арюна Александровна 

(Подпись, дата)

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

Студент Кунгурова Арюна Александровна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34461

Направление (специальность) 10.03.01. - Технологии защиты информации

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Создание плана КР	05.12.2023	04.12.2023	
2	Анализ литературы	08.12.2023	10.12.2023	
3	Составление основного текста КР	15.12.2023	15.12.2023	
4	Оформление отчета	16.12.2023	17.12.2023	
5	Защита КР	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Кунгурова Арюна Александровна 
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Кунгурова Арюна Александровна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34461

Направление (специальность) 10.03.01. - Технологии защиты информации

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом ☐ Сформулированы при участии студента ☒ Определены руководителем

Цель данной работы – повышение защищенности рассматриваемой организации за счет применения инженерно-технических средств защиты информации.

2. Характер работы

☐ Расчет ☐ Конструирование ☒ Моделирование ☐ Другое

3. Содержание работы

В данной курсовой работе рассмотрены организационная структура предприятия, обоснование защиты информации, анализ защищаемых помещений, анализ рынка существующих решений, проектирование плана расстановки средств технической защиты информации.

4. Выводы

В результате выполнения работы был произведен комплексный анализ возможных технических каналов утечки информации, а также предложены меры пассивной и активной защиты информации.

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Кунгурова Арюна Александровна 
(Подпись, дата)

«___»_____2023 г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время информационная безопасность приобрела внушительную экономическую и социальную значимость. Утечки информации наносят вред компаниям во всех сферах нашей жизни – от государственных учреждений до торговли. Такие риски могут привести к серьезным последствиям и большому ущербу, поэтому задача обеспечить комплексную защиту информации становится первостепенной для большинства предприятий.

Для создания надежной системы защиты информации должны применяться не только организационные меры, программно-аппаратные, криптографические средства, но и инженерно-технические средства защиты, так как именно они позволяют обеспечить отсутствие несанкционированного доступа к каналам связи, по которым в организации передается важная информация. Актуальность данной работы обусловлена необходимостью разработки эффективного способа противодействия утечкам с помощью технических средств защиты, ведь без них практически не могут быть достигнуты конфиденциальность и целостность информации.

Риск утечки данных может возникнуть вследствие как невнимательности сотрудников, так и преднамеренных действий злоумышленников. Для эффективного противодействия таким инцидентам, в первую очередь, необходимо выявить потенциальные угрозы проникновения на защищаемый объект, а также возможные каналы несанкционированного доступа к защищаемой информации. При выявлении технических каналов утечки информации необходимо учитывать все элементы защиты, включая основное оборудование, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы вентиляции.

В данной работе будет рассмотрена специфика процесса разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну.

Цель работы – повысить защищенность рассматриваемой организации за счет применения инженерно-технических средств защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ организационной структуры предприятия:
- обосновать необходимость защиты информации;
- провести анализ защищаемого помещения;
- провести анализ рынка и выбрать инженерно-технические средства защиты информации;
- спроектировать систему защиты информации на основе выбранных средств.

Практическая значимость работы заключается в дальнейшей возможности применения полученных в ходе разработки комплекса инженерно-технических сведений при проектировании системы защиты информации реального предприятия.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Рассматриваемая в данной работе организация занимается разработкой оборудования, применяемого в военных целях, сведения о которых относятся к государственной тайне. Факт обработки таких данных обуславливает введение усиленных мер по сохранению конфиденциальности и доступности информации.

Структура предприятия является иерархической и содержит 6 отделов. Схема представлена на рисунке 1.

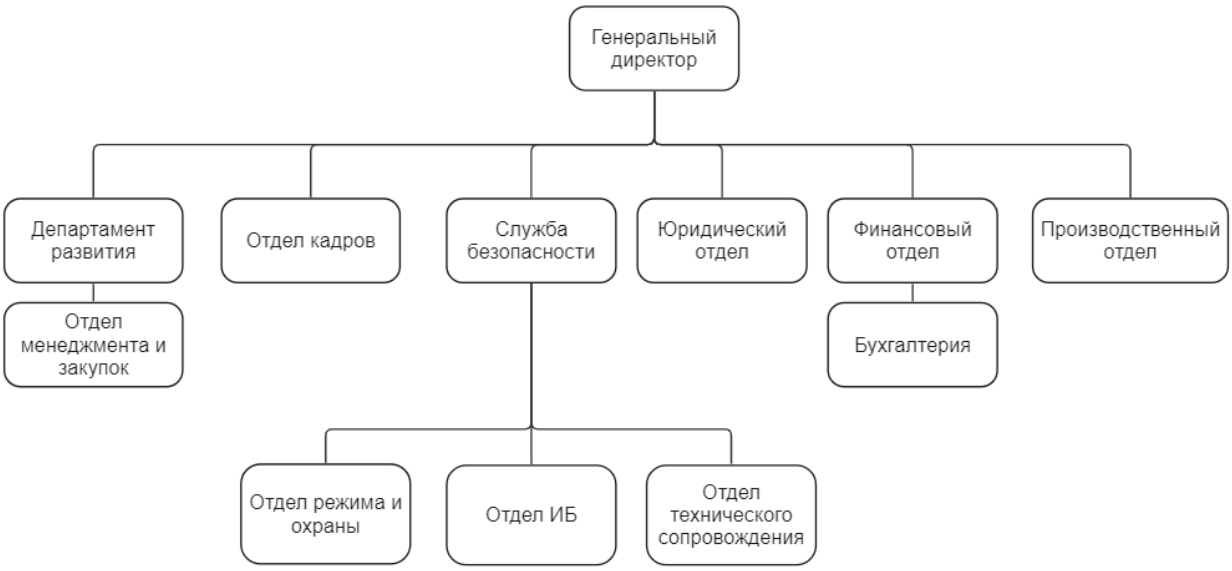


Рисунок 1 – Структура предприятия

Информационные потоки представляют собой передачу информации от одного источника к другому, целями которой являются обмен данными, улучшение коммуникации, обеспечение доступа к информации и обеспечение эффективного функционирования различных систем организации.

Порядок обработки информации обусловлен правилами внутреннего распорядка взаимодействия подразделений. Информационные потоки характеризуют работу предприятия, в том числе ее взаимодействие с другими организациями и частными лицами как по открытым, так и по закрытым каналам.

Схема информационных потоков представлена на рисунке 2.

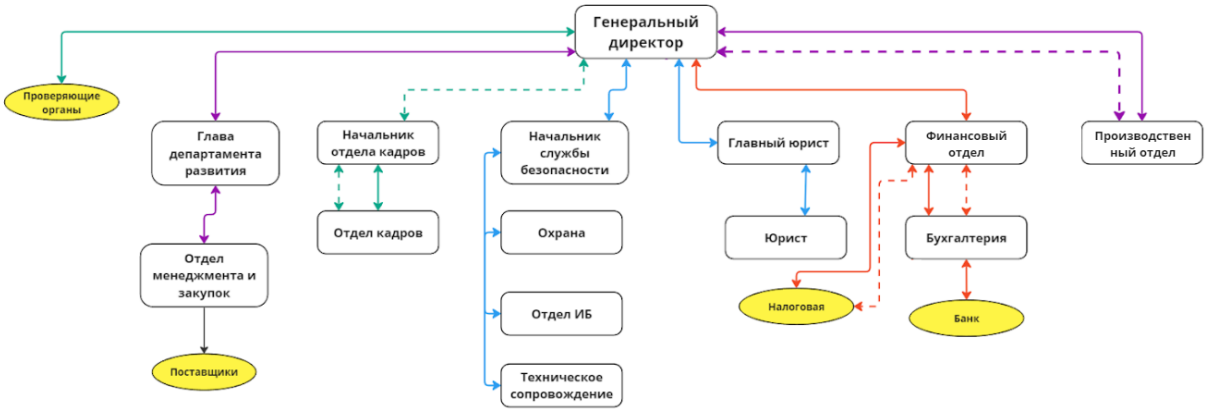


Рисунок 2 – Схема информационных потоков

Условные обозначения, использованные при составлении схемы, предоставлены в таблице 1.

Таблица 1 – Условные обозначения на схеме информационных потоков

Обозначение	Описание
	Внутренний субъект организации
	Внешний субъект
	Информация, связанная с обеспечением оптимального функционирования основной деятельности организации
	Информация, связанная с экономической деятельностью организации
	Информация, связанная с обеспечением информационной и физической безопасности организации
	Информация, связанная с основной деятельностью
	Информация, связанная с внешним взаимодействием
	Закрытые информационные потоки
	Открытые информационные потоки

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Необходимость наличия средств защиты информации, составляющей государственную тайну, регламентируется нормативными актами, регламентами и руководящими документами, представленными в следующем перечне:

1. Указ Президента РФ «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. No212.
2. Указ Президента РФ «Вопросы защиты государственной тайны» от 30.03.1994 г. No614.
3. Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. No1203.
4. Указ Президента РФ «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644.
5. Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 05.05.2012) «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».
6. Постановление Правительства РФ от 04.09.1995 N 870 (ред. от 22.05.2008) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».
7. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 01.11.2012) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».
8. Федеральный закон «О государственной тайне» от 21 июля 1993 г. No5151–1.
9. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. No24-ФЗ.
10. СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.

Государственная тайна — это сведения политического, экономического, военного и научно-технического характера, утрата или разглашение которых создает угрозу безопасности и независимости государства или наносит ущерб его интересам.

Установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

- особой важности;
- совершенно секретно;
- секретно.

По постановлению Правительства РФ от 4 сентября 1995 г. N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» к секретным сведениям следует относить все сведения, отличные от сведений:

− особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

− совершенно секретных: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

3 АНАЛИЗ ПЛАНА ПОМЕЩЕНИЯ

3.1 План защищаемого помещения

В ходе работы было рассмотрено помещение 1 из подразделений, так как отделы минимально различаются по планировке и обустройству.

В здании рассматриваемого предприятия располагаются 10 помещений. На рисунке 3 представлен план помещения.

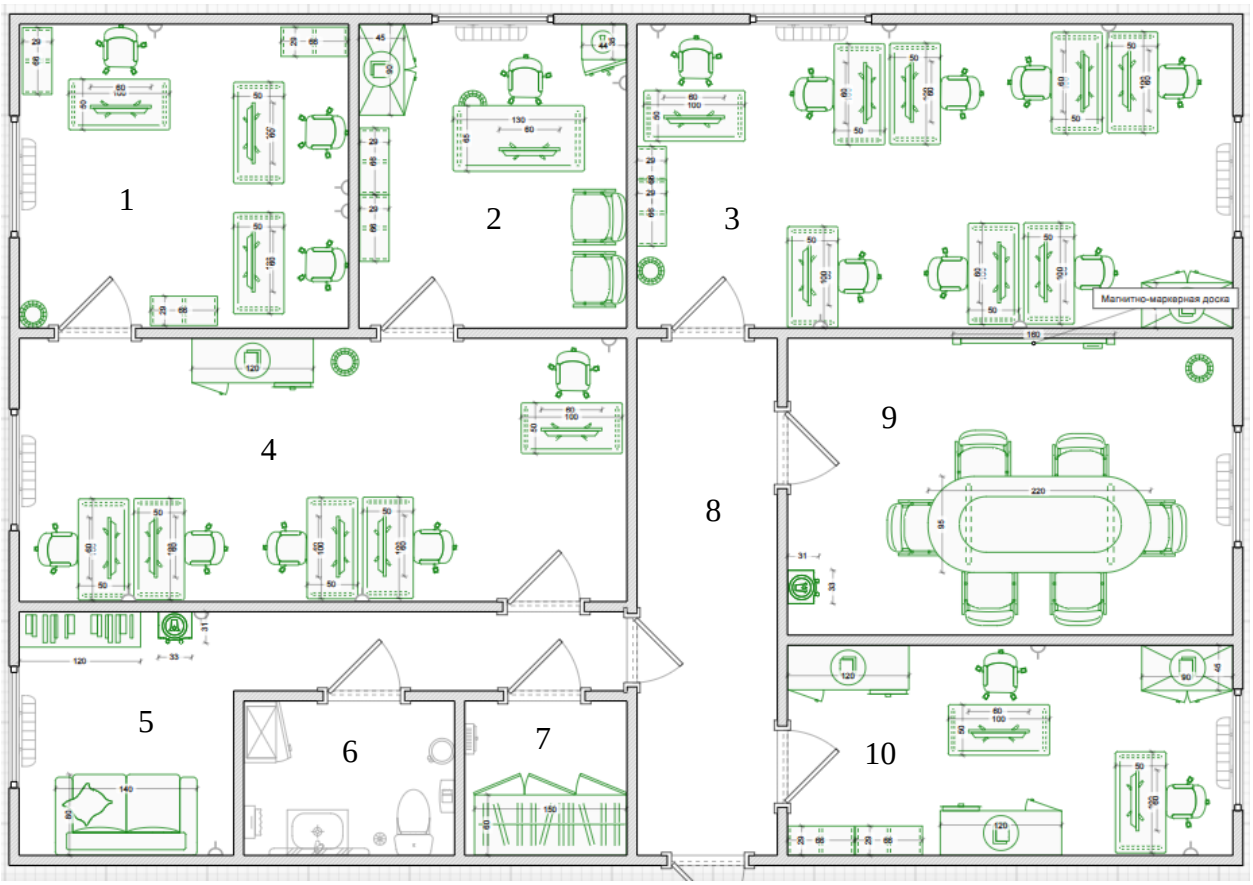
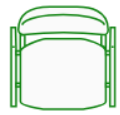
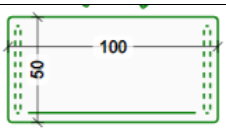
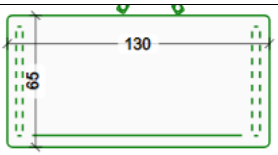
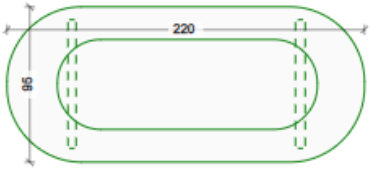
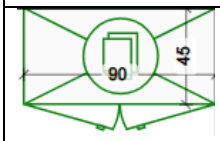
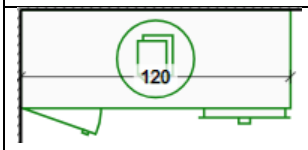
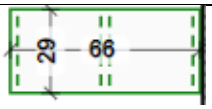
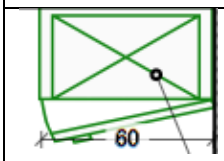
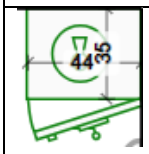
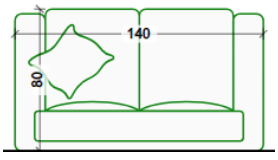
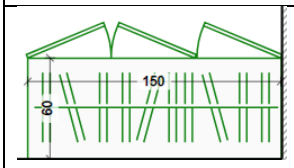


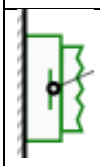
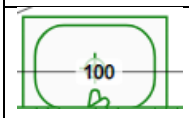
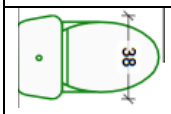
Рисунок 3 – План помещения

Условные обозначения представлены в таблице 2.

Таблица 2 – Условные обозначения плана помещения

Обозначение	Описание
	АРМ
	Кресло офисное

	Стул
	Рабочий стол
	Стол руководителя
	Стол для переговоров полукруглый
	Шкаф офисный
	Шкаф книжный
	Тумба
	Стеллаж
	Шкаф-пенал
	Сейф
	Диван
	Сервер

	Урна
	Урна туалетная
	Магнитно-маркерная доска
	Кулер
	Диспенсер для полотенец
	Диспенсер для туалетной бумаги
	Раковина с тумбой
	Зеркало
	Унитаз
	Ершик
	Электрощиток
	Радиатор
	Розетка

3.2 Описание помещений

Работа в защищаемом помещении подразумевает в основном работу с документами, содержащими государственную тайну, поэтому применение мер по защите информации является основополагающим. В таблице 3 представлены назначения помещений предприятия, а также их площадь.

Таблица 3 – Назначения помещений

Номер помещения	Назначение	Площадь, $м^2$
1	Помещение для персонала 1	9,78
2	Кабинет руководителя	7,96
3	Помещение для персонала 2	17,70
4	Рабочее помещение и приемная	15,63
5	Помещение для отдыха	8,14
6	Санузел	3,18
7	Серверная	2,45
8	Коридор	7,09
9	Помещение для проведения переговоров	12,92
10	Помещение для персонала 3	9,14

Описание наполненности помещений представлено в таблице 4.

Таблица 4 – Содержание помещений

Назначение	Содержание
Помещение для персонала 1	3 АРМ, 3 рабочих стола, 3 кресла офисных, 3 стеллажа, 1 урна, 3 розетки, 1 радиатор, 1 окно
Кабинет руководителя	1 АРМ, 1 стол руководителя, 1 кресло офисное, 1 урна, 1 сейф, 2 стула, 2 стеллажа, 1 шкаф офисный, 1 розетка, 1 радиатор, 1 окно
Помещение для персонала 2	8 АРМ, 8 рабочих столов, 8 кресел офисных, 2 стеллажа, 1 урна, 1 шкаф офисный, 5 розеток, 2 радиатора, 2 окна
Рабочее помещение и секретарь	5 АРМ, 5 рабочих столов, 5 кресел офисных, 1 тумба, 1 урна, 3 розетки, 1 радиатор, 1 окно
Помещение для отдыха	1 диван, 1 шкаф книжный, 1 кулер, 2 розетки, 1 радиатор, 1 окно
Санузел	1 шкаф-пенал, 1 унитаз, 1 раковина с тумбой, 1 зеркало, 1 диспенсер для туалетной бумаги, 1 диспенсер для полотенец, 1 ершик, 1 урна туалетная
Серверная	1 сервер, 1 электрощиток, 2 розетки
Помещение для проведения переговоров	1 стол для переговоров полукруглый, 6 стульев, 1 магнитно-маркерная доска, 1 кулер, 1 урна, 1 радиатор, 1 окно

Помещение для персонала 3	2 АРМ, 2 рабочих стола, 2 кресла офисных, 2 стеллажа, 2 тумбы, 1 шкаф офисный, 1 урна, 2 розетки, 1 радиатор, 1 окно

Защищаемое помещение расположено на 8 этаже 16-этажного здания, окружено смешанными предприятиями и офисами других организаций. На остальных этажах расположены офисы, магазины и небольшие предприятия. Слева от защищаемого помещения находится офис IT-компании, а справа – агентство по переводу. окна помещения не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания выполнены из железобетона и имеют толщину около 30 см. Во всех помещениях присутствует настенная, или потолочная вентиляция.

3.3 Анализ потенциальных каналов утечки информации

Для того, чтобы определить состав средств защиты информации, которые необходимо установить, сначала нужно выделить возможные каналы утечки информации, которые делятся на следующие типы.

− акустические (акустоэлектрические) – утечка по такому каналу возможна при прослушивании помещения со стороны соседних помещений через открытые окна и форточки с помощью направленных микрофонов, а также из-за закладных устройств, которые могут быть спрятаны в системах хранения или вентиляционных шахтах;

− вибрационные (виброакустические) – утечка через стекла, тонкие стены, радиаторы, любой твердый предмет, совершающий вибрации;

− электромагнитные (электрические) – утечки, связанные с электронными устройствами: АРМ, бытовая техника, а также розетки и проводка;

− визуально-оптические – утечка через открытые окна, прозрачные перегородки и незакрытые двери;

− материально-вещественные – хищение имущества, в рамках данной курсовой работы не рассматривается, так как подразумевается, что взаимодействие с физическими носителями информации строго регулируется политикой компании.

3.4 Выбор средств защиты

Средства защиты информации можно разделить на пассивные и активные. К пассивным средствам технической защиты относятся экранирующие устройства,

разделительные устройства в сетях электроснабжения, защитные фильтры и другие средства. Основная цель пассивного подхода заключается в максимальном ослаблении сигнала от источника информации. Например, это может достигаться за счет применения звукопоглощающих материалов при отделке стен или экранирования технических устройств.

В отличие от пассивных, активные технические средства защиты представляют устройства, способные создавать активные помехи (или их имитации) для средств технической разведки. Такие устройства могут также нарушать нормальное функционирование средств негласного сбора информации. Активные методы предупреждения утечки информации могут включать в себя обнаружение и нейтрализацию этих устройств.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна с грифом «секретно», требуется обеспечить помещение средствам защиты, приведенными в таблице 5.

Таблица 5 – Средства защиты для различных каналов утечки

Канал	Источник	Пассивная защита	Активная защита
Акустический (акустоэлектрический)	Вентиляционная шахта, проводка, открытые двери и окна, тонкие стены	Звукоизоляция, фильтры для сетей электропитания, закрытие окон и дверей при обсуждении важной информации	Устройства акустического зашумления
Вибрационный (виброакустический)	Радиаторы, трубы, тонкие стены, другие твердые поверхности	Изолирующие звук и вибрацию обшивки стен и пола	Устройства вибрационного зашумления
Электромагнитный (электрический)	Розетки, АРМ, техника	Фильтры для сетей электропитания, защитные экраны	Устройства электромагнитного зашумления
Визуально-оптический	Окна, двери	Жалюзи / шторы на окнах, тонирующие	Бликующие устройства

		пленки на окнах, доводчики на дверях	

4 АНАЛИЗ РЫНКА

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно».

Решение Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199 «Типовые нормы и правила проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», регламентирует следующие требования к защите помещений:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.

3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.

4. Все режимные помещения оборудуются аварийным освещением.

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

4.1 Защита от утечки информации по акустическим и виброакустическим каналам

Принцип работы канала основан на способности звуковой волны вызывать механические колебания в препятствиях (в т. ч. воздухе), через которые она проходит при распространении. Эти колебания при помощи оборудования преобразуются в связный

текст. Для снижения риска утечки информации по виброакустическому каналу требуется максимально ослабить акустический сигнал от источника звука, подающийся на коммуникации, служащие средой его распространения, где он может быть перехвачен.

Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

- усиленные двери;
- тамбурное помещение перед переговорной;
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления, т. е. необходимо сгенерировать в среде распространения сильный помеховый сигнал, который невозможно доступными злоумышленнику техническими средствами отфильтровать от информационного.

В таблице 6 приведен сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу.

Таблица 6 – Средства защиты информации от утечек по виброакустическому каналу

Устройство	Характеристика	Цена, ₽
Соната-АВ-4Б	Максимальное количество излучателей: 239 шт. Сертификат ФСТЭК Диапазон воспроизводимого шумового сигнала: 90–11200 Гц. Световая и звуковая индикация СПО «Камертон»	45 000
SEL-155 «Сонет»	Подключение до 50 генераторов-излучателей сигнала и гальванических размыкателей линий Диапазон воспроизводимого шумового сигнала: 90–11200 Гц Формирователь электрических сигналов маскирующих помех «белого шума» с шестиполосным (октавным) эквалайзером Светодиодный индикатор режима работы дополнительный регулятор общего уровня шумовой помехи	34 300
Камертон-5	Диапазон воспроизводимого шумового сигнала: 90–11200 Гц.	46 000

	Сертификация ФСТЭК Максимальное количество подключаемых модулей: ВД-80/ВД-120 = 4шт.; АС-Ш/АСП = 4шт Интерфейс управления: пленочная клавиатура + ЖК экран Индикация: световая, звуковая, ЖК	
ЛГШ-404	Диапазон рабочих частот175 –11200 Гц Сертифицирован ФСТЭК России по 2 классу защиты Возможность установки в ВП до 2 категории включительно Возможность подключения до 40 преобразователей	35 100
Буран	Диапазон воспроизводимого шумового сигнала: 100–11200 Гц Сертификат ФСТЭК 3 помеховых канала (виброакустических – 2, акустических – 1); Возможность подключения до 50 преобразователей	67 500

В ходе анализа была выбрана система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ-4Б», предназначенная для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам. К ее преимуществам относятся: наличие сертификата ФСТЭК, использование принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что дает возможность: создать систему автоматического контроля всех элементов и значительно снизить время на конфигурирование и тестирование системы.

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита сети 220 В заключается в использовании сетевых помехоподавляющих фильтров. Такие фильтры не пропускают информативные сигналы, возникающие при работе средств оргтехники. Причём, правильно установленный фильтр также защищает средства оргтехники от вредного влияния внешних помех. Следует учитывать, что для эффективной работы помехоподавляющих фильтров необходимо качественное заземление.

К активным методам защиты сети переменного тока (220 В) относятся методы, предусматривающие формирование специальными генераторами шумового сигнала, превосходящего по уровню сигналы устройств съёма информации или информативные сигналы. В таблице 7 представлены средства активной защиты от утечек по электрическому каналу.

Таблица 7 – Средства защиты информации от утечек по электрическому каналу

Устройство	Характеристика	Цена, ₽
ЛГШ-501	Сертифицирован ФСТЭК России по 2 классу защиты Визуальная система индикации нормального режима работы и визуально-звуковая система индикации аварийного режима Спектральная плотность напряжения шумового сигнала в диапазоне частот от 0,01 до 30 МГц 10-58 дБ Спектральная плотность напряжения шумового сигнала в диапазоне частот от 30 до 400 МГц 10-47 дБ Спектральная плотность напряженности электрического поля шума в диапазоне частот от 0,8 до 1000 МГц 20-75 дБ Спектральная плотность напряженности магнитного поля шума в диапазоне частот от 0,01 до 30 МГц 20-65 дБ Диапазон регулировки уровня – 20 дБ	29 900
Соната-РС3	Световая и звуковая индикация	32 400

	Регулировка уровня шума в 3 частотных полосах Диапазон частот: до 2 ГГц Сертификат ФСТЭК	
Генератор шума Покров	Диапазон шумового сигнала: для электрической составляющей 0,01–6000 МГц для магнитной оставляющей 0,01–30 МГц для электрических сигналов, наведённых на цепи электропитания 0,01–400 МГц Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления Сертификат ФСТЭК	32 800
ГШ-111П	Диапазон генерируемого шумового сигнала10 кГц – 3 000 МГц 2 независимых канала генерирования маскирующих помех с цифровыми многочастотными эквалайзерами регулировки уровней электромагнитного поля и электрических шумовых сигналов Интерфейс для управления и контроля ГШ по сети Ethernet 10/100 Мбит/с; Система управления и индикации	75 000
Штора (ПРП-2500)	Диапазон рабочих частот: 0,1-2500 МГц. Повышенная выходная мощность до 35 Вт Автономная работа до 50 минут Камуфлирован в сумку для видеокамеры	85 700

В ходе анализа средств защиты от утечки по виброакустическому каналу был выбран ЛГШ-501 преимущественно из-за относительно небольшой стоимости. Также можно выделить наличие сертификата ФСТЭК, возможность регулирования уровня излучаемых электромагнитных шумов, световой и звуковой индикаторы аварийного режима и контроля уровня излучения.

4.3 Устройства для перекрытия визуально-оптического канала утечки информации

Для снижения вероятности успешного использования злоумышленником оптического канала утечки информации необходимо установить на окно жалюзи, шторы или тонирующие пленки. С точки зрения удобства содержания были выбраны жалюзи.

Для избежания наблюдения через приоткрытую дверь, необходимо использовать доводчики, которые автоматически закрывают дверь после ее открытия.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

По результатам анализа в 4 главе данной работы, были выбраны следующие средства защиты информации:

- усиленные двери (минимум 4 мм, обшитые металлом минимум 2 мм со звукоизолирующей прокладкой на металлическом каркасе);
- виброакустическая защита Соната АВ-4Б;
- генератор шума Соната-РС3
- устройство активной защиты о ПЭМИН ЛГШ-501;
- жалюзи;
- дверные доводчики.

Необходимое количество генераторов-вибровозбудителей «СВ-4Б1» можно предварительно оценить из следующих норм:

- стены: 1 на каждые 3–5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол: 1 на каждые 15–25 м2 перекрытия;
- 1 на окно (при установке на оконный переплет);
- 1 на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо-, тепло- и газоснабжения – 1 на каждую вертикаль вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей «СА-4Б1» можно предварительно оценить из следующих норм:

- 1 на каждый вентиляционный канал или дверной тамбур;
- 1 на каждые 8–12 м3 надпотолочного пространства или других пустот.

Полная комплектация устройств представлена в таблице 8.

Таблица 8 – Оценка стоимости технических средств защиты

Тип средства	Наименование	Количество	Цена за 1 ед., ₽	Общая стоимость, ₽
Блок электропитания и управления	Соната-ИП4.3	1	21 600	21 600
Генератор-акустоизлучатель	СА-4Б1	11	7 440	81 840
Генератор-вибровозбудитель	СВ-4Б	57	7 400	421 800

Пульт управления комплексом	Соната-ДУ4.3	1	7 680	7 680
Размыкатель слаботочной линии	Соната-ВК4.2	4	6 000	24 000
Размыкатель линии Ethernet	Соната-ВК4.3	1	6 000	6 000
Генератор шума	ЛГШ-501	5	29 900	149 500
Жалюзи	Рулонная штора однотонная блэкаут "Белый"	8	1 966	15 728
Металлическая дверь	Rex 8	6	45 810	274 860
Итог	1 003 008			

Таким образом, итоговая сумма, необходимая для закупки инженерно-технических средств защиты информации, составила 1 003 008 рублей.

План помещения с установленными средствами технической защиты информации представлен на рисунке 4.

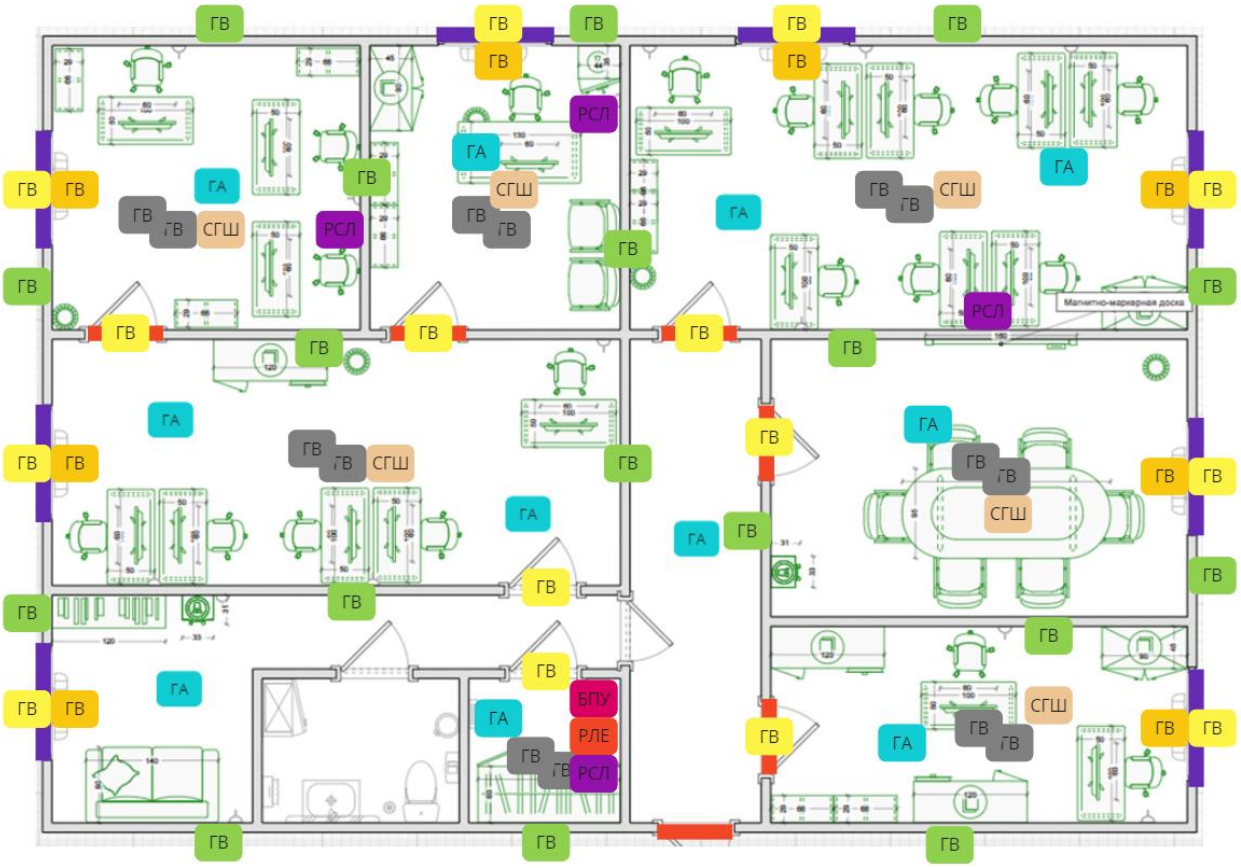


Рисунок 4 – План помещений со средствами защиты информации

Условные обозначения средств защиты информации, использованных при проектировании, представлены в таблице 8.

Таблица 8 — Условные обозначения средств защиты информации

Обозначение	Описание	Количество, шт.
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна)	15
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (стены)	18
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок)	14
ГВ	«Соната-СВ-4Б» генератор-вибровозбудитель (радиаторы, трубы)	10
ГА	Генератор-акустоизлучатель «Соната СА-4Б»	11

	Блок электропитания и управления «Соната-ИП4.3»	1
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	4
	Генератор шума «ЛГШ-501»	5
	Рулонная штора однотонная блэкаут "Белый	8
	Усиленная звукоизолирующая дверь Rex 8	6

ЗАКЛЮЧЕНИЕ

В ходе работы были рассмотрены основные аспекты обеспечения информационной безопасности с помощью различных инженерно-технических средств. Был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и были описаны необходимые меры, направленные на повышение защиты организации. Также был проанализирован рынок существующих технических средств для противодействия несанкционированному доступу через рассматриваемые каналы утечки информации и выбраны наиболее подходящие для нашего объекта средства. Был разработан план установки и произведен расчет сметы затрат, итоговое значение которой составило 1 003 008 рублей. Так как предприятие работает с государственной тайной, обеспечение конфиденциальности и целостности информации является первостепенной задачей, что оправдывает затраты.

Таким образом, в результате работы был предложен комплекс мер по защите от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному, техническим каналам защиты информации.

Знания о способах применения инженерно-технических средств защиты информации расширяют сферу компетенций специалиста по информационной безопасности и являются неотъемлемой частью требований для квалифицированного сотрудника.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кармановский Н. С., Михайличенко О. В., Савков С. В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.
2. Рекомендации по определению количества и мест установки акустоизлучателей и вибровозбудителей. / [Электронный ресурс] // : [сайт]. — URL: http://www.npoanna.ru/Content.aspx?name=recommendations.placement (дата обращения: 18.01.2024).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012 (дата обращения: 18.01.2024).
4. Оборудование для защиты информации // INFOSECUR URL: https://infosecur.ru/product/oborudovanie-dlya-zashchity-informatsii/ (дата обращения: 18.01.2024).