

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

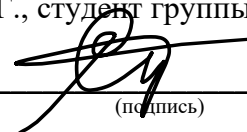
«Инженерно-технические средства защиты информации»

На тему:

«Разработка комплекса инженерно-технической защиты информации в помещении»

Выполнил:

Сергиенко С. Г., студент группы N34461


(подпись)

Проверил:

Попов Илья Юрьевич, 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	Сергиенко Сергей Григорьевич
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34461
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Канжелев Юрий Алексеевич, к.т.н., с.н.с., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении
Задание	Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

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

Содержание пояснительной записки

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

Рекомендуемая литература

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 с.

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Сергиенко Сергей Григорьевич
	(Подпись, дата)

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

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

Студент Сергиенко С.Г.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю., доцент, к. т. н.

(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	Заполнение титульных листов и поиск источников	29.09.2023	30.09.2023	
2	Анализ информации	29.09.2023	30.09.2023	
3	Написание курсовой работы	14.10.2023	14.10.2023	
4	Подготовка презентации	21.10.2023	21.10.2023	
5	Защита курсовой работы	28.10.2023	28.10.2023	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Сергиенко Сергей Григорьевич

(Подпись, дата)

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

Студент Сергиенко Сергей Григорьевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю., доцент, к. т. н.

(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

**2. Характер
работы**

☐ Расчет

☐

☐ Моделирование

Конструирование

Другое: Исследовательская
работа

3. Содержание работы

В ходе работы мы познакомимся с рынком инженерно-технических средств защиты информации, а также разработаем инженерно-техническую систему защиты информации

4. Выводы

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему защиты информации для предприятия «УглеБит». Также научился выделять организационную структуру, провёл анализ рынка решений, а также разработал итоговый план предприятия.

Руководитель

Попов Илья Юрьевич

(Подпись, дата)

Студент

Сергиенко Сергей Григорьевич

(Подпись, дата)



СОДЕРЖАНИЕ

Содержание	2
ВВЕДЕНИЕ	3
1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
2 ОСНОВНАЯ ЧАСТЬ	6
2.1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	7
3 РУКОВОДЯЩИЕ ДОКУМЕНТЫ	12
4 Организационная структура предприятия	19
5 Обоснование защиты информации	20
6 План организации	23
7 Анализ рынка	25
8 Итоговый план предприятия	33
Заключение.....	35
Список Использованных источников	36

ВВЕДЕНИЕ

Цель работы – повышение уровня защищенности рассматриваемого помещения.

Задачи:

- Проанализировать защищаемое помещение;
- Оценить каналы утечки информации;
- Проанализировать рынок;
- Выбрать меры пассивной и активной защиты информации;
- Представить результат работы в виде схемы с установленными средствами защиты.

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Коммерческая тайна – информация конфиденциального характера из любой сферы производственной и управленческой деятельности государственного или частного предприятия, разглашение которой может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем на основе государственных законодательных актов. Коммерческая тайна включает в себя также подробности коммерческой деятельности, состав партнеров, источники сырья, технологию сбыта продукции.

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Промышленная тайна – это новые технологии, открытия, изобретения, применяемые в процессе производства продукции, и т. д.

Финансовая тайна - бухгалтерские и финансовые документы, деловая переписка и т.д.

Личная тайна – это сведения конфиденциального характера, разглашение которых может нанести материальный ущерб отдельному (физическому) лицу. Охрана личной тайны осуществляется ее владельцем. Государство не несет ответственность за сохранность личных тайн.

Документ – представленная на материальном носителе информация с идентификатором, позволяющим установить характер документа и его собственника.

Источник речевой информации - разговоры в помещениях и системы звукоусиления и звуковоспроизведения.

Носитель видовой информации объекта - сам объект, а также его фото и видеоизображения на материальных носителях информации.

Политическая разведка - деятельность по добыванию сведений внутривнутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства.

Экономическая разведка - сбор сведений, раскрывающих экономический потенциал определенной страны.

Военная разведка - сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники.

Научно-техническая разведка – сбор сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

Агентурная разведка - добывание информации и проведения диверсионных акций специально подобранных, завербованных и профессионально подготовленных агентов. Легальная разведка-добыча информации при различных официальных связях и контактах с нашей страной, из легальных источников информации.

Техническая разведка - сбор информации с использованием технических разведывательных средств.

Воздушные каналы - каналы утечки информации, в которых средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Вибрационные каналы - каналы утечки информации, в которых средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

Акустоэлектрические каналы - каналы утечки информации, в которых утечка происходит за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами. Перехват акустических колебаний осуществляется через ВТСС, обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания».

Гидроакустический канал - канал, который образуется в водной среде и позволяет добывать акустическую информацию с использованием гидрофонов (сонаров).

Оптико-электронный канал - каналы утечки информации, в которых утечка образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т. д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация).

Параметрические каналы - канал, в котором в результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС.

2 ОСНОВНАЯ ЧАСТЬ

Чтобы построить эффективную систему предотвращения утечки информации в первую очередь необходимо определить потенциальные и реальные угрозы технологического проникновения на защищаемый объект, несанкционированного доступа и утечки защищаемой информации.

Эта работа основывается на знании физической природы возникающих технологических каналов утечки информации и методов технологической разведки. Правильная идентификация потенциальных угроз на предварительных этапах проекта по созданию системы защиты от промышленного шпионажа позволит в дальнейшем выбрать наиболее подходящие контрмеры и защитные меры.

При выявлении технических путей утечки информации необходимо комплексно рассмотреть основное оборудование технических средств обработки информации, соединительные линии, силовые распределительные и коммутационные устройства, системы электроснабжения, системы вентиляции и другие элементы защиты. Помимо основных технических средств, непосредственно связанных с обработкой и передачей конфиденциальной информации, необходимо учитывать вспомогательные технические средства и системы (ВТС), такие как технические средства открытой телефонной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часовые системы, электроприборы и другие. Наибольшее внимание следует уделять вспомогательным средствам, линии которых находятся за пределами контролируемой зоны, а также посторонним линиям и кабелям, проходящим через помещения, где установлено основное и вспомогательное техническое оборудование, металлические трубы, системы отопления, водоснабжения и другие токопроводящие металлические конструкции.

При оценке защищенности объекта от утечек аудиоинформации следует учитывать возможность подслушивания с соседних объектов или улиц. Следует оценить возможность разведки с помощью лазерных микрофонов. Интерес могут представлять каналы утечки из-за вибрации, вызванной звуковым давлением твердых тел (заборы, трубы и т.д.).

Цель защиты информации от шпионажа техническими средствами на конкретном объекте разведки определяется конкретным перечнем потенциальных угроз. В общем случае цели защиты информации могут быть сформулированы следующим образом:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется своевременностью, активностью, непрерывностью и комплексностью. Крайне важно реализовать комплексные меры защиты, то есть перекрыть все опасные каналы утечки информации.

Следует помнить, что эффективность системы защиты снижается при наличии хотя бы одного не закрытого канала утечки.

2.1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Существует три формы утечки информации:

- разглашение информации;
- несанкционированный доступ к информации;
- утечка информации по техническим каналам.

В рамках данной работы рассматривается только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Основными объектами защиты информации являются:

- информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией:

- средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

- технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т. д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления. Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют объект ТСПИ.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;

- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Далее полученная информация преобразуется в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал (усиление) и преобразует информацию в форму сигнала, доступную получателю (человеку или техническому устройству).

По физической природе носителя и виду канала связи ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;
- акустоэлектрические;
- виброакустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Информацию можно получить с помощью наблюдения, например, заглядывая в окна или полуоткрытые двери. Еще одним вариантом является использование

оборудования, позволяющего делать фотографии или видеозаписи. Этот канал утечки также подходит для графического отображения информации и защищен использованием жалюзи или других непрозрачных покрытий на видимых снаружи поверхностях (например, окна, стеклянные двери) и использованием доводчиков.

Радиоэлектронные каналы утечки информации используют в качестве носителей электрические, магнитные и электромагнитные поля в радиочастотной области и токи (поток электронов), распространяющиеся по металлическим проводам. Электромагнитный ТКУИ связан с перехватом электромагнитного излучения, генерируемого на частотах систем передачи и коммуникационного оборудования. Он используется для перехвата информации, передаваемой по радиосвязи, радиорелейной и спутниковой связи. Напряженность поля в точке приема (перехвата) прямо пропорциональна мощности передатчика и высоте приемо-передающей антенны и обратно пропорциональна расстоянию. Этот путь утечки актуален, когда в помещении находятся телефоны, компьютеры и другое оборудование для обработки информации. Электромагнитное излучение, возникающее при работе технического оборудования, называется электромагнитным случайным излучением и индукцией (ЭМИ) и защищается специальными техническими устройствами, которые генерируют электромагнитный шум для маскировки этого излучения.

Электрический ТКУИ относится к извлечению информации путем контактного подключения несанкционированного оборудования к кабельным линиям связи. Электрические колебания, создаваемые электроприборами, содержат информацию о подключенном оборудовании. Защита обеспечивается специальными фильтрами для сетей электропитания, которые скрывают электрические колебания, генерируемые вычислителем.

Индуктивный ТКУИ относится к бесконтактному извлечению информации из кабелей связи. Возможность такого извлечения информации обусловлена наличием вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальными индуктивными датчиками, усиливается и демодулируется в устройстве нарушителя. Бесконтактные закладные устройства - самые сложные для обнаружения устройства, поскольку они не изменяют характеристики канала связи. Такая защита обеспечивается за счет использования специального программного или аппаратного обеспечения, способного обнаружить встраивание.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Методы получения информации включают подслушивание снаружи помещения (при отсутствии звукоизоляции) и закладку устройств с возможностью записи голоса. Этот канал утечки актуален там, где информация передается голосом (например, диалоги, совещания) и защищена использованием звукоизоляционных материалов, не позволяющих звуку проникать наружу, или применением специального программного или аппаратного обеспечения, способного обнаружить имплантацию.

В акустоэлектрическом канале информация представляется в виде акустических колебаний, которые воздействуют на сеть электропитания и вызывают электрические колебания. Когда эти колебания удаляются, исходный акустический сигнал может быть восстановлен. Этот путь утечки информации актуален при наличии в контролируемом помещении электрической сети, связанной с внешним миром. Например, телефонные линии. Подавая небольшое напряжение на входящую телефонную линию и снимая его на входе, можно получить акустическую информацию, которая может распространяться по всему помещению. Защита достигается путем использования специальных фильтров в сети электропитания для маскировки колебаний, вызванных ударами по электрической сети.

В виброакустическом канале информация сначала представляется в виде акустических колебаний, которые при ударе о какую-либо твердую поверхность преобразуются в виброакустические колебания. Этот путь утечки информации чаще всего является актуальным, поскольку связан с твердыми поверхностями контролируемых помещений, такими как стены, потолки, полы, отопительные панели и оконные стекла.

Защита достигается за счет использования специальных технических устройств, которые передают белый шум на защищаемую твердую поверхность, делая вибрации, вызванные акустическими волнами, невидимыми. Под материальными каналами понимается утечка информации в результате несанкционированного распространения материальных носителей, содержащих защищенную информацию, за пределами контролируемой территории. К материальным носителям часто относятся рукописи, использованная копировальная бумага и портативные носители информации (карты памяти HD, SS и другие). Борьба с кражей и копированием информации, записанной на материальных носителях, ведется в основном с помощью организационных мер и введения строгих процедур учета и обращения с этими носителями.

3 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Проведём анализ существующих РПД. Так как наше предприятие работает с государственной тайной, то рассмотрим документы, которые относятся к гос тайне.

1.Законы Российской Федерации:

«О государственной тайне» от 21 июля 1993 г. N 5485–1 (последняя редакция).

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Государственную тайну составляют:

1. сведения в военной области:
 - о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
 - о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
 - о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
 - о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
 - о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;
2. сведения в области экономики, науки и техники:
 - о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о

размещении, фактических размерах и об использовании государственных материальных резервов;

- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

- **Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну**

- Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

- Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

- **Статья 30. Контроль за обеспечением защиты государственной тайны**

- Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

2.Указы Президента Российской Федерации:

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.

В соответствии со статьей 4 Закона Российской Федерации "О государственной тайне" постановляю:

1. Утвердить прилагаемый перечень сведений, отнесенных к государственной тайне.
2. Правительству Российской Федерации организовать работу по приведению действующих нормативных актов в соответствие с перечнем сведений, отнесенных к государственной тайне.
3. Настоящий Указ вступает в силу со дня его подписания.

«О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.

В соответствии с Законом Российской Федерации "О государственной тайне" постановляю:

1. Образовать Межведомственную комиссию по защите государственной тайн
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.**

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:

Утвердить прилагаемый перечень сведений конфиденциального характера.

3. Постановления Правительства Российской Федерации:

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921-51.

Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства РФ.

Защита осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путём проведения специальных работ, порядок организации и выполнения которых определяется Правительством РФ

Главными направлениями работ по защите информации являются:

- Обеспечение эффективного управления системой защиты информации
- Определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения
- Анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите

- Разработка организационно-технических мероприятий по защите информации и их реализация

- Организация и проведение контроля состояния защиты информации

Основными организационно-техническими мероприятиями по защите информации являются:

- Лицензирование деятельности предприятий в области защиты информации

- Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности

- Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам

- Введение территориальных, частотных, энергетически, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

- Создание и применение информационных и автоматизированных систем управления в защищенном исполнении

- Разработка и внедрение технических решений и элементов защиты информации при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи

- Разработка средств защиты информации и контроля за её эффективностью (специального и общего применения) и их использование

- Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи

«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» от 15 апреля 1995 г. №333.

В соответствии с Законом Российской Федерации "О государственной тайне" и в целях установления порядка допуска предприятий, учреждений и организаций к 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, Правительство Российской Федерации постановляет:

1. Утвердить Положение 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 (прилагается).

3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

4. Установить, что предприятия, учреждения и организации, допущенные к моменту принятия настоящего постановления к работам, связанным с использованием сведений, составляющих государственную тайну, могут осуществлять эти работы в течение 1995 года.

7. Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются - руководители предприятий), и при выполнении следующих условий:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

«О внесении дополнения в Положение 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» от 30 апреля 1997 г. №513.

В связи с созданием в Министерстве обороны Российской Федерации системы сертификации средств защиты информации, предусмотренной постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (Собрание законодательства Российской Федерации, 1995, N 27, ст. 2579), Правительство Российской Федерации постановляет :

Дополнить абзац третий пункта 2, абзацы второй и пятый пункта 10 Положения 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, утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 г. N 333 (Собрание законодательства Российской Федерации, 1995, N 17, ст. 1540; 1996, N 18, ст. 2142), после

слов: "Служба внешней разведки Российской Федерации" словами: "Министерство обороны Российской Федерации".

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.

1. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

2. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

3. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.

4. К совершенно секретным сведениям следует относить сведения 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.

5. К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. 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-разыскной области деятельности.

«О сертификации средств защиты информации» от 26 июня 1995 г, №608.

В соответствии с Законами Российской Федерации "О государственной тайне" и "О сертификации продукции и услуг" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение о сертификации средств защиты информации.

2. Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Федеральной службе безопасности Российской Федерации и Министерству обороны Российской Федерации в пределах определенной законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующие положения о системах сертификации, перечни средств защиты информации, подлежащих сертификации в конкретной системе сертификации, а также по согласованию с Министерством финансов Российской Федерации порядок оплаты работ по сертификации средств защиты информации.

1. Настоящее Положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические

(шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации).

Системы сертификации создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются - федеральные органы по сертификации).

4 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Для проектирования инженерно-технической системы защиты информации на предприятии мы должны провести анализ общих сведений данного предприятия.

Наименование организации: «УглеБит»

Область деятельности: Разработка, ремонт БПЛА-разведчиков и восстановление данных с поврежденных установленных носителей информации.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа: Рисунок 1

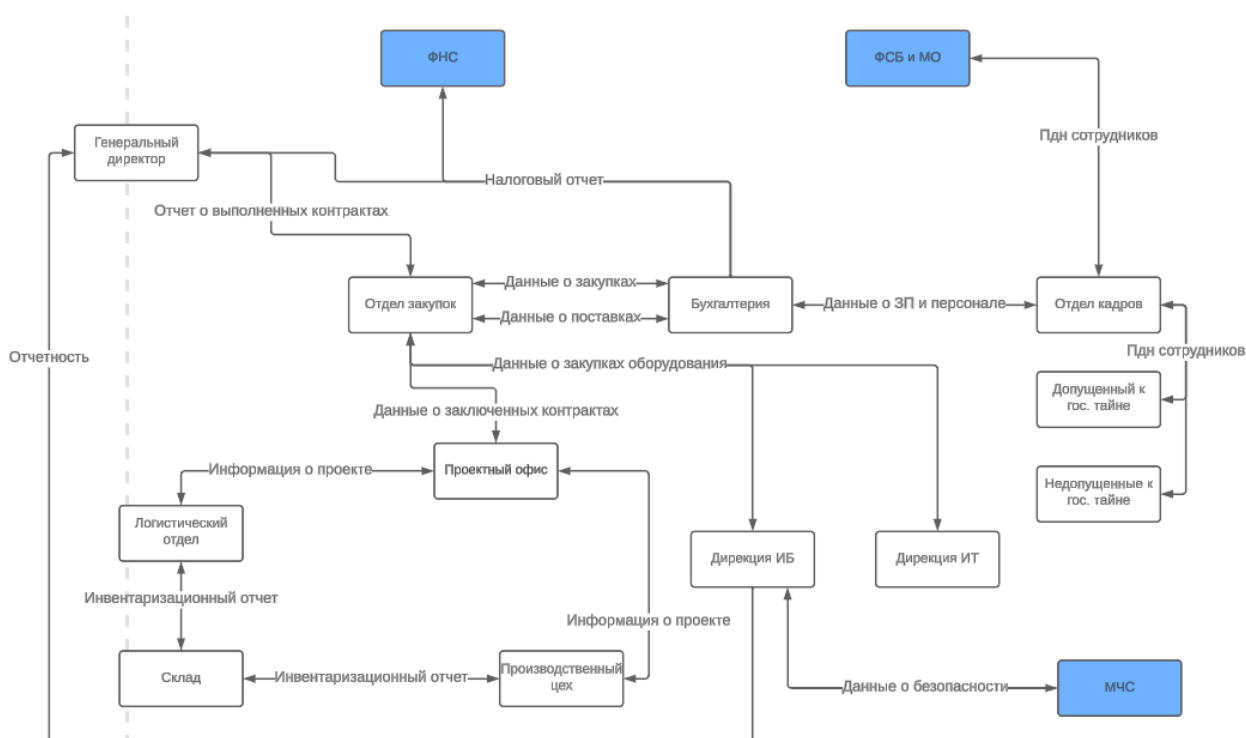


Рисунок 1 – Информационные потоки организации

5 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. No212;
- «Вопросы защиты государственной тайны» от 30.03.1994 г. No614;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. No1203;
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. No1108;
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. No71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. No573, от 14 июня 1997 г. No594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. No188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- Инструкция No0126–87;
- Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам
- Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. No921–51;
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. No1233;
- «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» от 15 апреля 1995 г. No333;

– «О внесении дополнения в Положение 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» от 30 апреля 1997 г. No513;

– «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. No870;

– «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. No973;

– «О сертификации средств защиты информации» от 26 июня 1995 г, No608.

На сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

– СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;

– СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;

– Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;

– Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;

– Временный порядок аттестации объектов информатизации по требованиям безопасности информации;

– Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

– Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;

– Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования;

– Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;

– Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Относящиеся законы Российской Федерации:

– «О государственной тайне» от 21 июля 1993 г. No5151–1;

– «Об информации, информатизации и защите информации» от 20 февраля 1995 г. No24-ФЗ;

– «О безопасности» от 5 марта 1992 г. No2446–1;

– «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. No4524–1;

– «О связи» от 16 февраля 1995 г. No15-ФЗ;

– «Об участии в международном информационном обмене» от 4 июля 1996 г. No85-ФЗ.

6 ПЛАН ОРГАНИЗАЦИИ

Проанализируем план предприятия (рисунок 2)

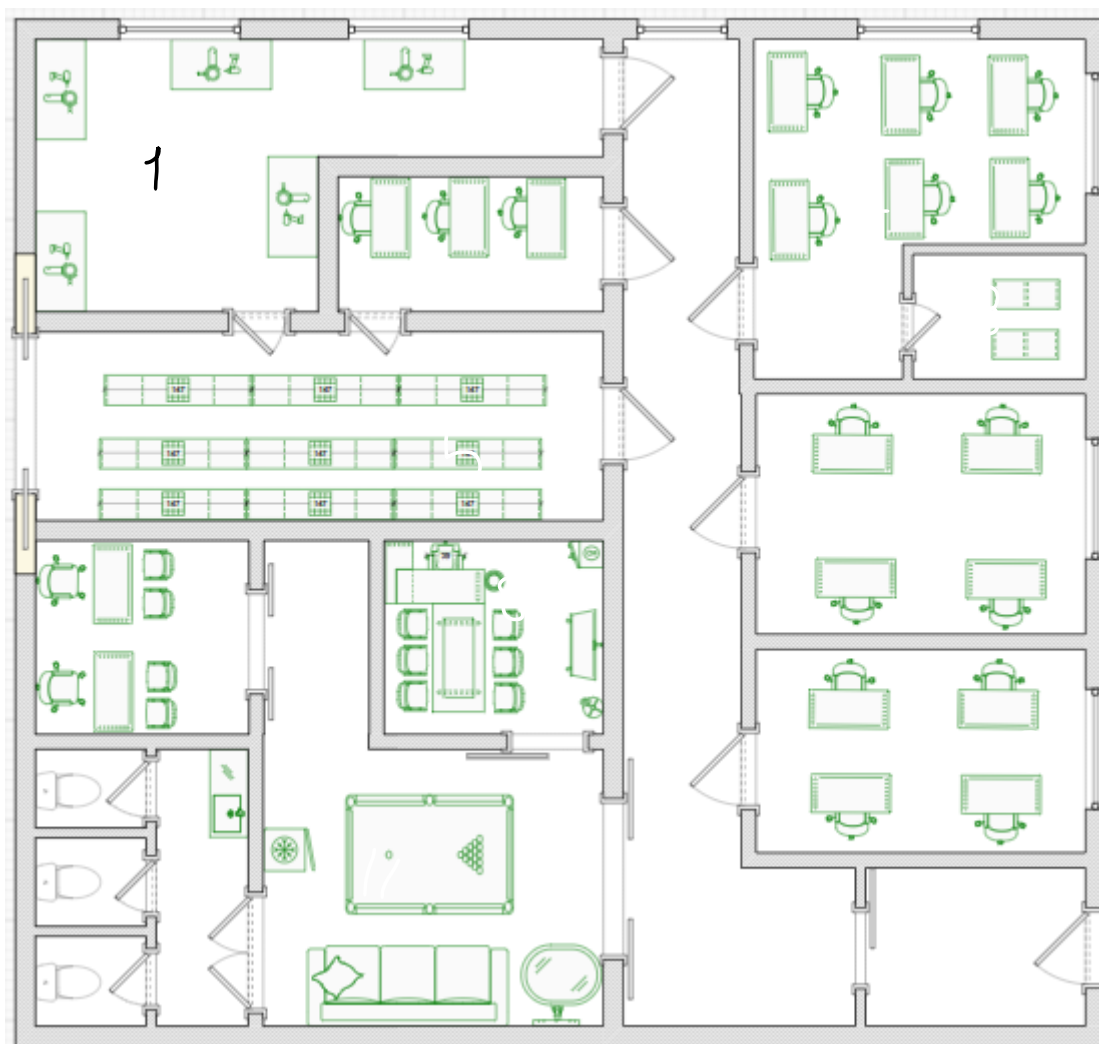


Рисунок 2 – План предприятия

Легенда:

1. Технический цех
2. ИБ
3. Серверная
4. Отдел закупок
5. Склад
6. Информационный цех
7. Проектный офис
8. Кабинет главного директора / переговорная
9. Бухгалтерия и отдел кадров

- 10. Уборная
- 11. Зона отдыха
- 12. КПП

7 АНАЛИЗ РЫНКА

В данном разделе произведем анализ рынка решений по инженерно-технической защите информации.

Выберем подходящие решения, которые подходят к нашим каналам утечки и напишем им описание.

1. Блокираторы беспроводной и сотовой связи:

- Блокираторы беспроводной связи предназначены для блокирования работы устройств несанкционированного получения информации, работающих в стандартах сетей сотовой связи и в стандартах Bluetooth и WiFi.

- Принцип работы заключается в генерации шумовой помехи в необходимом диапазоне частот. При этом возможна плавная регулировка мощности помехового сигнала в каждом из диапазонов, что позволяет обеспечить блокирование беспроводных стандартов связи только в границах защищаемого помещения.

2. Акустическое зашумление:

- Система постановки акустических помех предназначена для противодействия специальным средствам несанкционированного съема информации, использующим в качестве канала утечки воздушную среду помещения. К ним относятся: микрофоны и диктофоны.

3. Виброакустическое зашумление:

- Система постановки виброакустических помех предназначена для противодействия специальным средствам несанкционированного съема информации, использующим в качестве канала утечки ограждающие конструкции помещения. К ним относятся:

1. Электронные или акустические стетоскопы для прослушивания через потолки, полы и стены
2. Проводные или радиомикрофоны, установленные на ограждающие конструкции или водопроводные и отопительные трубопроводы;
3. Лазерные или микроволновые системы съема информации через оконные проемы помещений.
4. Защита сети 220/380В:

- Сети переменного тока содержат в себе двойную опасность. Во-первых, это утечка акустической информации по сети переменного тока (220 В). Во-вторых, угроза утечки информативных сигналов средств оргтехники.

- Существуют пассивные и активные методы защиты сети переменного тока (220 В) от несанкционированного съема информации.

- 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.

5. Пространственное зашумление:

- При работе самых различных устройств (например, вычислительной техники) могут появляться сигналы ПЭМИН (побочные электромагнитные излучения и наводки), содержащие обрабатываемую информацию конфиденциального характера. Эти сигналы могут быть перехвачены с помощью специальной аппаратуры.

- Генераторы радиопомех предназначены для работы в составе систем активной защиты информации (САЗ), обеспечивая защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.

6. Защита слаботочных линий и линий связи:

- Слаботочных линий и линий связи содержат в себе угрозу утечки акустической информации по ним. Устройства оказывают противодействие прослушиванию/расшифровке переговоров.

Теперь анализируем рынок (таблица 1) исходя из наших решений

Категория	Наименование устройства	Краткое описание	Цена
Блокираторы беспроводной и сотовой связи:	ЛГШ-718	Блокиратор сотовой связи ЛГШ-718 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах: IMT-MC-450, GSM900, DSC/GSM1800, (DECT1800), IMT-2000/UMTS (3G), 4G-2600 (LTE, WiMAX), Bluetooth, WiFi. Эффективный радиус подавления 3.50 м	114400руб.
	ЛГШ-715	Блокиратор беспроводной связи стандартов IMT-MC-450, GSM900, DSC/GSM1800, (DECT1800), IMT-2000/UMTS (3G) Эффективный радиус подавления 3.50 м	74620 руб.
	ЛГШ-701	Блокиратор сотовой связи стандартов: IMT-MC-450 GSM900 DSC/GSM1800 Эффективный радиус подавления 3.50 м	97500
Акустическое зашумление:	ЛГШ-404	- Сертифицирован ФСТЭК России по 2 классу защиты - Возможность установки в ВП до 2 категории включительно	35100 руб.

		- Возможность подключения до 40 преобразователей	
	ЛГШ-303	Изделие «ЛГШ-303» мобильно и предназначено для работы в помещениях, (автомобилях) и других местах не требующих стационарных средств защиты информации по прямому акустическому каналу и не оборудованных стационарными источниками питания.	15600
	ЛГШ-304	Изделие «ЛГШ-304» соответствует: - типу «Б» средства акустической защиты информации с активным (содержащим в своей конструкции индивидуальный задающий источник шума) преобразователем, питаемым по линии вторичного электропитания от центрального блока питания. Изделие «ЛГШ-304» соответствует требованиям «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) – по 2 классу защиты.	25 220 руб.

Виброакустическое зашумление:	ЛГШ-404	- Сертифицирован ФСТЭК России по 2 классу защиты - Возможность установки в ВП до 2 категории включительно - Возможность подключения до 40 преобразователей	35100 руб.
	ЛГШ-402	Изделие «ЛГШ-402» соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными (не содержащими в своей конструкции индивидуальные задающие источники шума требующие электропитания) преобразователями.	18200 руб.
Защита сети 220/380В:	ЛГШ-221	Изделие «ЛГШ-221» является средством активной защиты информации (тип Б) от утечки за счет наводок информативного сигнала на цепи заземления и электропитания, выходящие за пределы контролируемой зоны. Изделие «ЛГШ-221» соответствует требованиям по безопасности информации, установленным в документе «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и	36400 руб.

		наводок» (ФСТЭК России, 2014) – по 2 классу защиты, может применяться в выделенных помещениях до 2 категории включительно.	
	ЛППФ-40-1Ф	Сетевой помехоподавляющий фильтр «ЛППФ-40-1Ф» является средством пассивной специальной защиты технических средств от утечки информации за счет наводок, т.е. преобразования излучения технических средств в электрический сигнал в сети электропитания, выходящей за пределы контролируемой зоны. Предельное значение тока, при котором допускается эксплуатация изделия 40 А	70200 руб.
Пространственное зашумление	ЛГШ-501	Изделие «ЛГШ-501» является: - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»); - средством активной защиты информации от наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.	29900 руб.

	ЛГШ-516СТАФ	<p>Изделие «ЛГШ-516СТАФ» соответствует 2 классу защиты.</p> <p>Изделие «ЛГШ-516СТАФ» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) с учетом изменений, внесенных приказом ФСТЭК России № 028 от 28.11.2019.</p>	51000 руб.
	ЛГШ-503	<p>Изделие «ЛГШ-503» является:</p> <ul style="list-style-type: none"> - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»); - средством активной защиты информации от наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны. 	44200 руб.
	ЛГШ-513	<p>Изделие «ЛГШ-513» соответствует:</p> <ul style="list-style-type: none"> - типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений; - типу «Б» - средства активной 	39000 руб.

		<p>защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.</p> <p>Изделие «ЛГШ-513» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.</p>	
Защита слаботочных линий и линий связи	Гранит-8	Назначение фильтра пропускать сигналы в речевом диапазоне частот при нормальном режиме работы телефонной линии и ослаблять высокочастотные сигналы, которые могут подаваться в линию при высокочастотном навязывании.	4160 руб.
	ЛУР-2	Размыкатель слаботочных линий питания	5590
	ЛУР-4	Размыкатель слаботочных линий Телефон	
	ЛУР-8	Размыкатель слаботочных Ethernet	

8 ИТОГОВЫЙ ПЛАН ПРЕДПРИЯТИЯ

В данном разделе мы спроектировали инженерно-техническую систему защиты информации на предприятии «УглеБит» (рисунок 3).

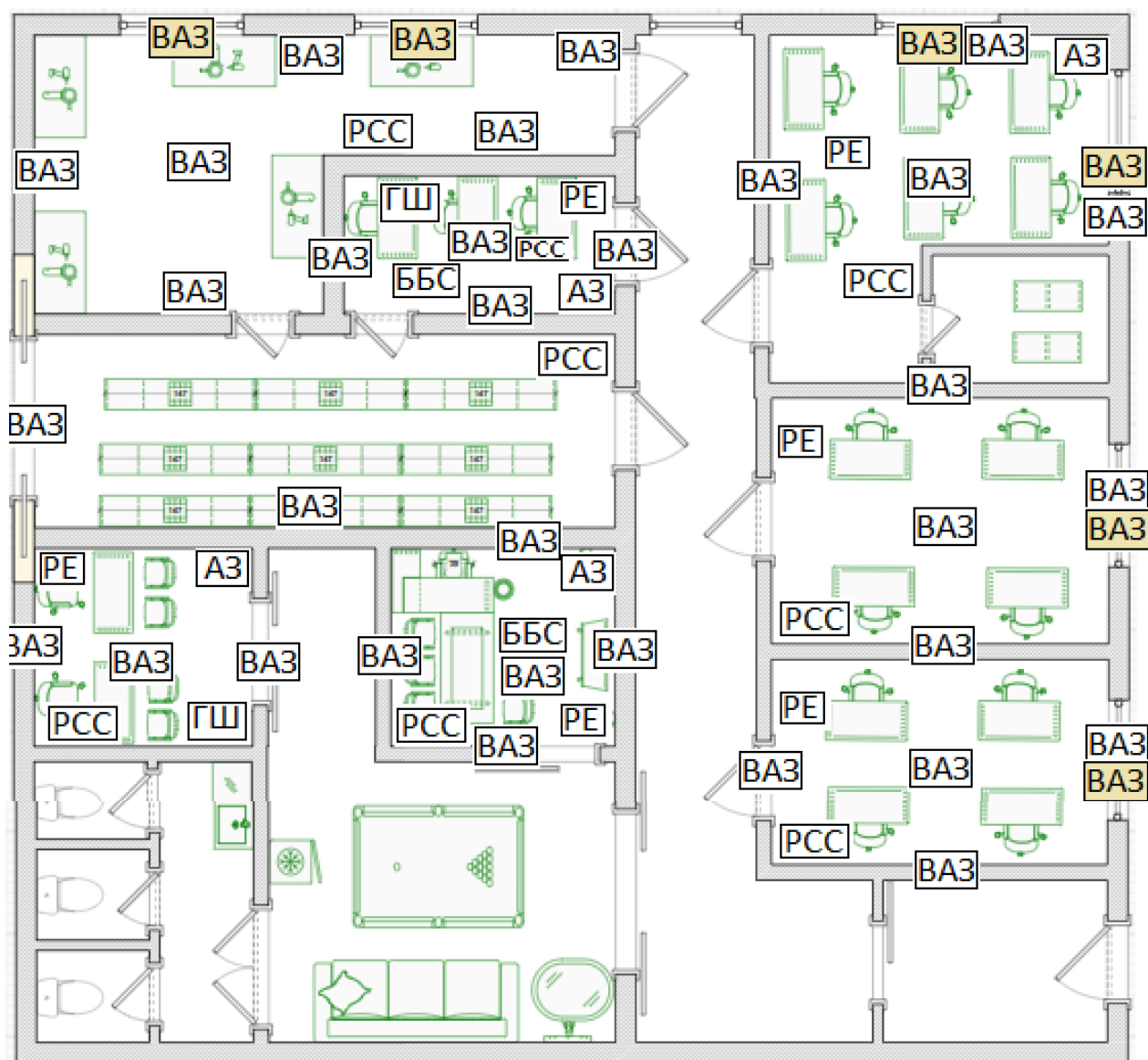


Рисунок 3 – Инженерно-техническая система защиты информации

Легенда:

- АЗ - Система акустических помех;
- ББС - Блокиратор беспроводной связи;
- ВАЗ - Система постановки виброакустических помех;
- ГШ - Генератор шума ПЭМИ;
- РСС - Размыкатель слаботочных сетей;
- РЕ - Размыкатель Ethernet;

- СГШ - Сетевой генератор шума;
- СФ - Сетевой помехоподавляющий фильтр;

ЗАКЛЮЧЕНИЕ

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему защиты информации для предприятия «Энигма», которая занимается разработкой специализированного программного обеспечения для ведения секретных операций и сбора разведывательной информации. Также научился выделять организационную структуру, провёл анализ рынка решений, а также разработал итоговый план предприятия.

Цель работы достигнута, все задачи выполнены

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)