

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

**«Инженерно-технические средства защиты
информации»**

На тему:

**Проектирование инженерно-технической защиты
информации на предприятии**

Вариант 36

Выполнил:



Савичев С. А.,

студент группы N34471

Проверил преподаватель:

Попов И. Ю., доцент ФБИТ

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Савичев Сергей Андреевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

Задание Разработать систему инженерно-технической защиты информации на предприятии

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, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



23.12.2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Савичев Сергей Андреевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	15.11.2023	18.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.2023	29.11.2023	
4	Представление выполненной курсовой работы	19.12.2023	23.12.2023	

Руководитель _____

(Подпись, дата)

Студент _____

23.12.2023

(Подпись, дата)

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

Студент Савичев Сергей Андреевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Цель данного исследования заключается в усилении общей безопасности рассматриваемого помещения. В процессе работы поставлена задача не только провести глубокий анализ уровня безопасности и выявить потенциальные угрозы информационной безопасности, но и разработать комплекс мер для укрепления как пассивных, так и активных методов защиты данных. Этот подход направлен не только на повышение степени защиты помещения, но и на создание гибких и адаптивных решений, способных успешно противостоять современным вызовам в области безопасности.

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое Проектирование

Содержание работы

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

3. Выводы

В процессе проведения исследования были выявлены общие стратегии по предотвращению утечки важной информации через технические каналы на предприятии. При рассмотрении вопросов кибер- и физической безопасности было подчеркнуто, что стратегии защиты должны постоянно эволюционировать и

интегрировать передовые методы предотвращения. Вывод заключается в необходимости не только использования современных технологических решений, но и активного формирования внутренней культуры безопасности в организации. Это включает в себя систематическое обучение сотрудников и их активное участие в процессах обеспечения безопасности. Такой комплексный и адаптивный подход становится неотъемлемой частью эффективной стратегии обеспечения безопасности в условиях современного информационного общества, где динамичность и непредсказуемость являются стандартом.

Руководитель

Студент



(Подпись, дата)

23.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

Введение	7
1 Организационная структура предприятия	8
1.1 Анализ технических каналов утечки информации	8
1.2 Информационные потоки	13
1.3 Перечень руководящих документов	14
1.4 Структура информационных потоков на предприятии	17
2 Обоснование защиты информации	18
3 Анализ защищаемых помещений	21
3.1 Схема помещения	21
3.2 Описание помещений	24
3.3 Анализ возможных каналов утечки информации	26
4 Анализ рынка технических средств	26
4.1 Выбор средств защиты	26
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	28
4.3 Защита от утечки информации по (вибро-) акустическим каналам....	30
4.4 Защита от ПЭМИН.....	33
4.5 Защита от утечек информации по оптическим каналам	36
5 Описание расстановки технических средств	37
Заключение	43
Список использованных источников	44

ВВЕДЕНИЕ

Средства обеспечения информационной безопасности представляют собой совокупность устройств и технических систем, включая инженерно-технические, электрические, электронные, оптические и прочие приспособления, приборы, а также другие элементы, предназначенные для решения разнообразных задач по защите информации. Эти задачи включают в себя предотвращение утечек, защиту от несанкционированного доступа (НСД) и обеспечение общей безопасности защищаемой информации.

В представленном исследовании разработан комплекс инженерно-технических средств защиты информации, содержащей государственную тайну с классификацией "секретно". Эта система создана для офиса, включающего девять помещений, из которых три подлежат обработке государственной тайны (кабинет директора, переговорная комната, первый отдел).

В ходе работы был проведен анализ технических каналов возможной утечки информации, а также рассмотрены требования к организации защиты режима секретности. Были изучены различные средства технической защиты информации, выбраны наиболее подходящие из них, и разработана схема монтажа и установки выбранных средств с целью обеспечения эффективной защиты информации.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Анализ технических каналов утечки информации

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Согласно теме курсовой работы, рассматриваться будет 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.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала,

представляющего собой носитель с информацией от её источника.

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.

Информация от источника поступает на вход канала на языке источника, поэтому полученную информацию передатчик преобразует 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. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съём информации;
- съём информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.



Рисунок 2 – Классификация технических каналов утечки информации

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Акустические ТКУИ в свою очередь делятся на акустоэлектрическом, виброакустическом и акустические.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей

используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с

функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействуют на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещении есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технических устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве

вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

1.2 Информационные потоки

Информационный поток представляет собой совокупность передаваемых сообщений в логистической системе, служащих для эффективного управления, анализа и контроля логистических операций на предприятии. Корректное управление и обеспечение безопасности информационных потоков играют важную роль в обеспечении конфиденциальности, целостности и доступности данных.

Эти потоки могут представляться разнообразными формами, включая бумажные и электронные документы, аудиозаписи, символы и сигналы. Основное деление информационных потоков на открытые и закрытые производится в зависимости от их цели.

Открытые информационные потоки доступны всем сотрудникам и заинтересованным сторонам в пределах предприятия без ограничений. Эти потоки включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Открытые потоки способствуют эффективному внутреннему обмену информацией, создавая атмосферу открытости и прозрачности.

В свою очередь, закрытые информационные потоки содержат

конфиденциальную и чувствительную информацию, требующую повышенного уровня защиты. Эти потоки включают в себя финансовые данные, персональные записи, интеллектуальную собственность и другую конфиденциальную информацию, которая при попадании в неправильные руки может повлечь серьезные последствия для предприятия. Защита закрытых потоков включает строгие политики доступа, шифрование данных и другие меры безопасности, направленные на обеспечение безопасности конфиденциальной информации.

1.3 Перечень руководящих документов

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. №212;
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108;
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

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

являются:

- инструкция №0126–87;
- 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. №921–51;
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;
- «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;
- «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;
- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;
- «О сертификации средств защиты информации» от 26 июня 1995 г. №608.

Также 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;
- 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.

Также, необходимо обратить внимания на законы Российской Федерации:

- «О государственной тайне» от 21 июля 1993 г. №5151–1;
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ;
- «О безопасности» от 5 марта 1992 г. №2446–1;
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1;
- «О связи» от 16 февраля 1995 г. №15-ФЗ;
- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

1.4 Структура информационных потоков на предприятии

На схеме информационных потоков (рисунок 3) зеленым цветом обозначены открытые потоки, включающие в себя бухгалтерскую и финансовую отчетность, а также налоговые сведения. Закрытые потоки, выделенные красным цветом, содержат важную защищаемую информацию, такую как персональные данные клиентов и сотрудников, служебная и коммерческая тайны, а также сведения о разрабатываемом программном продукте, включая программный код, его назначение и другие характеристики.

3. Согласно требованиям безопасности для 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, крепящейся к железным конструкциям оконного проема в стене;

4. Все режимные помещения оснащаются аварийным освещением;

5. Оборудование помещений для работы с государственной тайной должно соответствовать требованиям технической безопасности. Вся используемая аппаратура, периферийные устройства и программное обеспечение должны быть сертифицированы и соответствовать стандартам безопасности, установленным ФСТЭК;

6. Перед вводом в эксплуатацию выделенных и других режимных помещений необходимо провести проверку на наличие "жучков" и других средств несанкционированного получения информации. Подобные проверки следует проводить периодически для исключения возможности утечки информации.

Согласно Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники.

Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В» (таблица 1).

Таблица 1 – Классы защищенности автоматизированных систем

<p>Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные

Продолжение таблицы 1

<p>Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)</p>	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
<p>Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Для размещения технических средств защиты на объекте необходимо провести анализ защищаемого помещения, представленного на плане офисного типа предприятия (рисунок 4). В таблице 2 представлено описание

обозначений, использованных на плане.

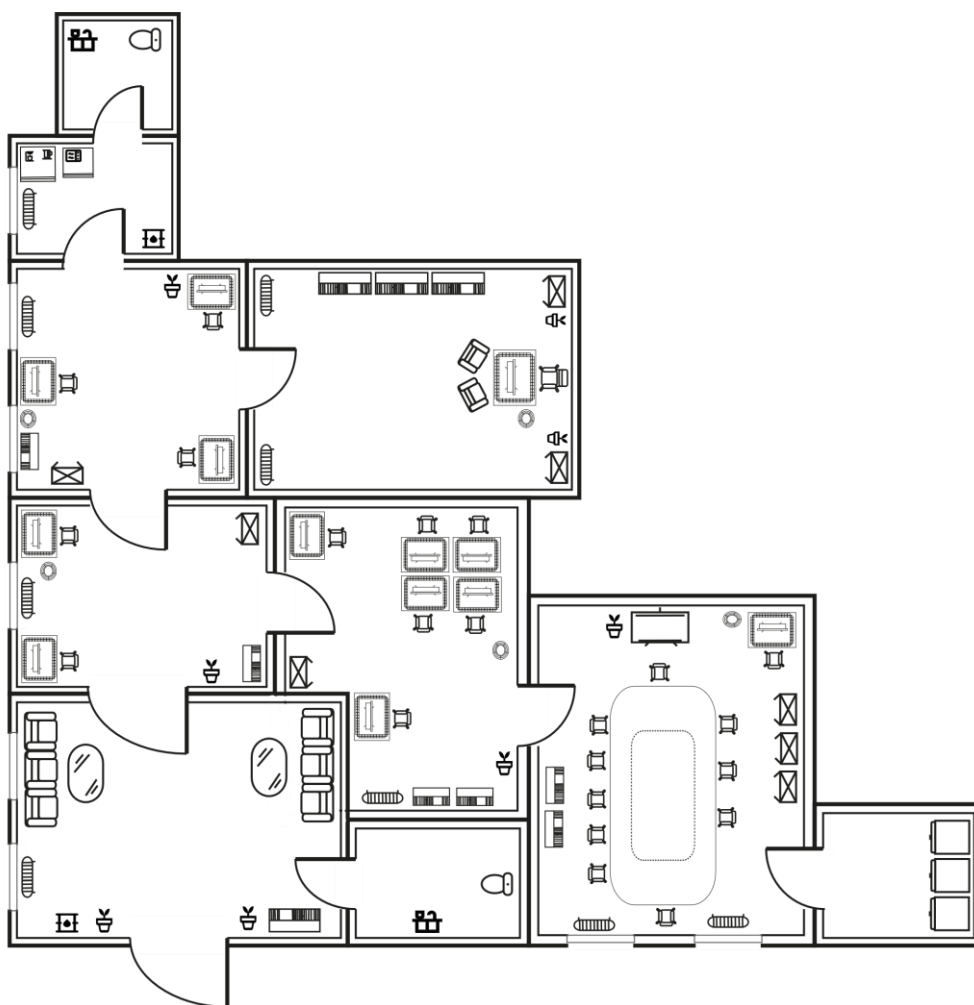


Рисунок 4 – План защищаемого помещения

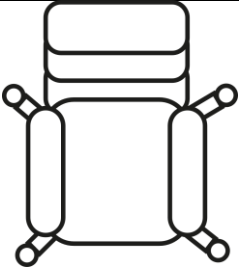
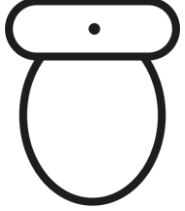
Таблица 2 – Описание обозначений

Обозначение	Описание
	Интерактивная доска с проектором
	Журнальный стол
	Книжная полка

Продолжение таблицы 2

Обозначение	Описание
	Комнатное растение
	Компьютер
	Компьютерный стол
	Кофе машина
	Кресло
	Кулер для воды
	Кухонный стол
	СВЧ-печь
	Сервер
	Стол переговоров

Продолжение таблицы 2

Обозначение	Описание
	Стул руководителя
	Унитаз

3.2 Описание помещений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- кабинет директора (20,2 м²);
- переговорная комната (22,1 м²);
- офис 1 (15,4 м²);
- офис 2 (18,1 м²);
- офис 3 (14,5 м²);
- серверная комната (9,7 м²);
- кухня (9,6 м²);
- главный холл (17,1 м²).

Кабинет директора включает в себя: один стул руководителя, два стула, один компьютерный стол, три книжных шкафа, два шкафа для документов, одно мусорное ведро для бумаги, два радиатора отопления и два комнатных растения. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся одиннадцать стульев, один стол для переговоров, один компьютерный стол, один компьютер, два книжных шкафа, три шкафа для документов, одна интерактивная доска с проектором, одно

мусорное ведро для бумаги, два радиатора отопления, два окна и одно комнатное растение. Переговорная комната оснащена восьмью розетками.

Офис 1, офис 2 и офис 3 предназначены для сотрудников предприятия.

В офисе 1 стоят два стула, два компьютерных стола, два компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и одно комнатное растение. В данном помещении находятся шесть розеток.

В офисе 2 есть шесть стульев, шесть компьютерных столов, шесть компьютеров, два книжных шкафа, один шкаф для документов, одно мусорное ведро для бумаги и одно комнатное растение. Данное помещение оснащено двенадцатью розетками.

В офисе 3 находятся три стула, три компьютерных стола, три компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, два окна и одно комнатное растение. Офис 3 оснащен восьмью розетками.

В серверной комнате расположены три сервера. В данном помещении есть девять розеток.

В кухне есть кулер для воды и кухонный стол, на котором находятся одна кофемашина, одна микроволновая печь и один чайник. Данное помещение включает в себя пять розеток.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся два по три кресла (совмещенных), два журнальных стола, один книжный шкаф, один кулер для воды, один радиатор отопления, два комнатных растения и два окна.

Окна помещения выходят в закрытый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется

сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 13 см.

3.3 Анализ возможных каналов утечки информации

В каждом помещении существуют потенциальные маршруты для нежелательной утечки информации, связанные с электромагнитными и электрическими протечками, такими как использование компьютеров и розеток. Декоративные элементы, вроде комнатных растений, могут служить средствами для установки подслушивающих устройств, которые способны передавать информацию через акустический канал.

Существует также риск утечки информации через оптические каналы, например, из-за незакрытых окон или незащищенных дверей. Необходимо также учитывать виброакустический канал, который может использоваться для передачи информации через твердые поверхности, такие как стены или батареи отопления.

Существует возможность вещественно-материального канала утечки информации из-за наличия материальных носителей данных, однако этот канал не может быть полностью заблокирован с использованием технических средств защиты.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 3. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений
Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов
Визуально-оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Защитные экраны и фильтры для сетей электропитания
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитного зашумления	Защитные экраны и фильтры для сетей электропитания

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

Пассивная защита в данном контексте включает в себя установку фильтров в электропитании всех помещений, направленных на минимизацию возможных электромагнитных и электрических утечек информации.

Система активной защиты основана на использовании белого шума в сети. Эта система генерирует постоянный фоновый шум, который маскирует колебания, возникающие от звуковых волн или работы электронных устройств. Для более детального анализа представлены модели устройств и их характеристики в таблице 4. Эти меры активной защиты направлены на обеспечение дополнительного уровня безопасности и предотвращение возможных технических каналов утечки информации в защищаемых помещениях.

Таблица 4 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ФСПК-10	42 550	Ток нагрузки – 10 А. Уровень шума/затухания – 80 дБ. Напряжение – 220 В. Частотный диапазон – 0,125 - 1000 МГц. Тип соединения – подключение к однофазным цепям электропитания с заземляющим проводом.	Сертифицировано ФСТЭК России. Устройство защиты речевой информации от утечки по 1-фазным электросетям. Количество фильтруемых проводов – 3. Температура эксплуатации – от +1 до +40С. Максимально допустимая сила тока в сети – 10А. Класс энергобезопасности – I (ГОСТ Р 12.1.019–2009 ССБТ).
Генератор шума ЛГШ-221	36 400	Ток нагрузки – сеть ~220 В +10%/-15%, 50 Гц. Напряжение – 220 В. Количество фаз – 1. Потребляемая мощность 10 Вт.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта. Сертифицировано ФСТЭК.

Продолжение таблицы 4

Модель	Цена, руб.	Характеристики	Особенности
ФСП-3Ф-15А-ИН	49 500	Ток нагрузки – 15 А. Уровень шума/затухания – 60–80 дБ. Напряжение – 380/220В 50Гц. Частотный Диапазон – 0,15–1000 МГц. Количество фаз – 1. Тип соединения – 5-проводное исполнение (3 фазы + заземление + изолированный нейтральный проводник).	Трехфазный сетевой фильтр, предотвращающий утечку наводок и информативных сигналов по сети. Выравнивает напряжение на входе, повышает помехоустойчивость подключенного оборудования. Есть модификация со сниженным реактивным током утечки фазы. Сертификат ФСТЭК, сертификация по ИСО, ГОСТ.

На основании анализа, проведенного в таблице 4, был выбран генератор шума ФСПК-10. Оптимальный вариант, так как устройство имеет класс энергобезопасности – I. К тому же генератор шума ФСПК-10 имеет сертификацию ФСТЭК, что является основополагающим фактором в выборе данного устройства.

4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности охватывают установку тамбурной зоны

перед переговорной комнатой и усиление дверей для дополнительной защиты. Для обеспечения звукоизоляции переговорной комнаты и офиса руководителя применяются специализированные материалы, способствующие снижению звуковой проницаемости стен и, таким образом, повышению конфиденциальности обсуждаемой информации.

Активные меры безопасности включают в себя систему виброакустической маскировки. Для обеспечения безопасности помещения, где обрабатывается информация с уровнем секретности "совершенно секретно", рассматриваются технические средства активной защиты информации, соответствующие категории не ниже 1Б (таблица 5). Эти меры направлены на предотвращение возможных технических каналов утечки информации, обеспечивая дополнительный уровень безопасности в защищаемых помещениях.

Таблица 5 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
SEL SP-157 Шагренъ	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Соната АВ-4Б	44 200	<p>Диапазон воспроизводимого шумового сигнала 175– 11200 Гц. Выходное напряжение В $12,5 \pm 0,5$. Электропитание сеть ~220 В/50 Гц.</p>	<p>Комплект состоит из блоков электропитания и управления, генераторов- акустоизлучателей, генераторов- вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.</p>

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Камертон–5	46 000	<p>Электропитание от сети. электропитание СВАЗ «Камертон-5» исп.2 осуществляется от сети переменного тока частотой 50 Гц с напряжением от 187 В до 242 В, по отдельным компонентам.</p> <p>Индикация – световая, звуковая, ЖК</p>	<p>Предназначено для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов.</p>

Исходя из анализа, представленного в таблице 5, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для предотвращения утечек информации через акустические и вибрационные каналы, данное устройство выделяется как наиболее востребованное, получившее положительные отзывы, и обладающее оптимальным соотношением цена-качество.

4.4 Защита от ПЭМИН

ПЭМИН – побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации. Зашумление обеспечивается типами генераторов, представленными в таблице 6.

Таблица 6 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ПОКРОВ	32 800	Наличие регулировки уровня шума. Диапазон частот – 0,01–6000 МГц (для изделия, выпускаемого по ВСЦТ.464214.003 ТУ). Электропитание – выполнен в виде сетевого удлинителя с 5 розетками типа F. Мощность – 15 Вт. Режим работы – круглосуточно.	Предназначен для защиты информации от утечки по техническим каналам за счет ПЭМИН путем излучения в окружающее пространство электромагнитного поля шумового сигнала и наводок на линии электропитания и заземления. Является средством активной защиты информации от утечки за счет ПЭМИН типов "А" и "Б", соответствует требованиям ФСТЭК России по 2 классу (сертификат №3757 от 09.06.2017). Сертификат ФСТЭК, СП

Продолжение таблицы 6

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ЛГШ- 513	39 000	Наличие регулировки уровня шума. Диапазон частот 10 кГц - 1800 МГц. Уровень шума от 0 до - 30 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А.	Сертификат ФСТЭК. Устройство соответствует: типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений и типу «Б» - средства активной 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

Продолжение таблицы 6

Модель	Цена, руб.	Характеристики	Особенности
SEL-155 «СОНЕТ»	39 800	Наличие регулировки уровня шума. Диапазон частот от 0,01 до 1800 МГц. Уровень шума до 32 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А. Мощность 30 Вт для управляющего блока.	Сертификат ФСТЭК. Защита речевой информации тип «Б» по 2 классу. Также система предназначена для защиты телефонных линий, линий компьютерных сетей, соединительных линий систем оповещения и сигнализации от утечки по каналу акустоэлектрических преобразований

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «ЛГШ-513». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

4.5 Защита от утечек информации по оптическим каналам

Для предотвращения функционирования оптического канала утечки информации можно применить следующие меры:

- тонированные пленки на стеклах;
- жалюзи;
- шторы на окна.

Наиболее приемлемым вариантом защиты является использование жалюзи на окнах, так как они не только блокируют возможность визуального наблюдения, но и эффективно защищают от солнечных лучей.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «ФСПК-10»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-513» от ПЭМИН
- жалюзи на восемь окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15...25 м² перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину

дверной коробки);

– трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

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

В таблице 7 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 7 – Необходимое оборудование



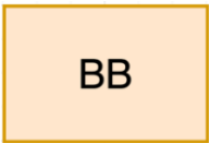
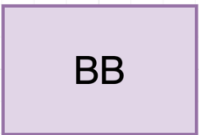
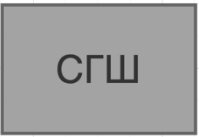




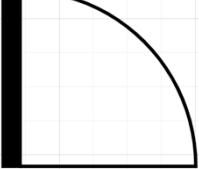
Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «ФСПК-10»	42 550	1	42 550
Генератор шума «ЛГШ- 513»	39 000	3	117 000
Блок электропитания и управления «Соната- ИП4.3»	21 600	1	21 600
Генератор- акустоизлучатель «Соната СА-4Б1»	3 540	15	53 100
Генератор- вибровозбудитель «Соната СА-4Б»	7 440	86	639 840
Рызмыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000


Продолжение таблицы 7

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель линии «Ethernet» «Соната ВК4.1»	6 000	1	6 000
Шторы-плиссе Blackout	4 900	8	39 200
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			1 188 147

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «ФСПК-10» и «ЛГШ-513» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 8 приведены описание обозначений устройств.

Продолжение таблицы 8

Обозначение	Устройство	Количество, шт.
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	31
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	16
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	35
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	4
	Сетевой генератор шума «ФСПК- 10»	1
	Генератор шума «ЛГШ-513»	3
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3

	Шторы-плиссе BlackOut	8
---	-----------------------	---

ЗАКЛЮЧЕНИЕ

В рамках данной курсовой работы были выполнены следующие задачи: определение структуры и информационных потоков компании, занимающейся обработкой данных с государственной тайной уровня "секретно". Также проведен анализ помещения для выявления возможных путей утечки информации. На основе исследования рынка технических средств защиты информации была составлена смета, включающая рекомендованные устройства для установки на предприятии. Таким образом, разработана комплексная система защиты, направленная на минимизацию возможных утечек по выявленным каналам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. – 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).